Journal of Network and Computer Applications 174 (2021) 102886

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

IoMT amid COVID-19 pandemic: Application, architecture, technology, and security

Azana Hafizah Mohd Aman [a,*], Wan Haslina Hassan [b], Shilan Sameen [b,c], Zainab Senan Attarbashi [d], Mojtaba Alizadeh [e], Liza Abdul Latiff [f]

[a] *Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Malaysia*
[b] *Malaysia-Japan International Institute of Technology, Universiti Teknologi Malaysia, Malaysia*
[c] *Directorate of Information Technology, Koya University, Koya, Kurdistan Region, Iraq*
[d] *School of Computing, Universiti Utara Malaysia, Malaysia*
[e] *Department of Computer Engineering, Lorestan University, Iran*
[f] *Fakulti Teknologi & Informatik Razak, Universiti Teknologi Malaysia, Malaysia*

ARTICLE INFO

Keywords:
COVID-19 pandemic mitigation
IoMT application
IoMT architecture
IoMT security
IoMT technology

ABSTRACT

In many countries, the Internet of Medical Things (IoMT) has been deployed in tandem with other strategies to curb the spread of COVID-19, improve the safety of front-line personnel, increase efficacy by lessening the severity of the disease on human lives, and decrease mortality rates. Significant inroads have been achieved in terms of applications and technology, as well as security which have also been magnified through the rapid and widespread adoption of IoMT across the globe. A number of on-going researches show the adoption of secure IoMT applications is possible by incorporating security measures with the technology. Furthermore, the development of new IoMT technologies merge with Artificial Intelligence, Big Data and Blockchain offers more viable solutions. Hence, this paper highlights the IoMT architecture, applications, technologies, and security developments that have been made with respect to IoMT in combating COVID-19. Additionally, this paper provides useful insights into specific IoMT architecture models, emerging IoMT applications, IoMT security measurements, and technology direction that apply to many IoMT systems within the medical environment to combat COVID-19.

1. Introduction

According to the World Health Organization (WHO, 2020), the novel **Co**rona**v**I**rus** **D**isease of 20**19**, otherwise known as COVID-19, is of the genus beta coronavirus and is related to the viruses that cause Severe Acute Respiratory Syndrome (SARS) and Middle Eastern Respiratory Syndrome (MERS). The first COVID-19 case was reported on December 31, 2019, was found in Wuhan, Hubei Province, China. Alarmed by the rate of infection and the level of severity of COVID-19, WHO classified the disease as a pandemic by March 2020. Since then, the coronavirus outbreak has reached 2,959,929 confirmed cases globally (at the time of writing), with 202,733 confirmed deaths affecting 213 countries (WHO, 2020).

COVID-19 shares nearly 80% sequence identity with SARS-CoV (Zhou et al., 2020). The results of (Sokouti et al., 2020) even show similarities between some parameters for both diseases in terms of recovery rates, mortality, and incidence. Therefore, existing approaches and treatments are useful in producing COVID-19 therapeutics (Yao et al., 2020). Based on SARS and MERS disease experience, WHO has issued comprehensive online technical guidance to all countries on how to detect and manage cases. WHO and its global partners have collaborated to accelerate the development of crucial health technologies. The group agreed that innovative COVID-19 diagnostics, therapeutics, and vaccines are required to sustain health systems.

Internet of Medical Things (IoMT) systems are increasingly diverse and prevalent and are excellent candidates for preventing, predicting, and monitoring emerging infectious diseases (Christaki, 2015; Alabdulatif et al., 2019) like COVID-19. The use of IoMT as a health monitoring system provides real-time surveillance through the use of wearable health-monitoring devices, Wireless Body Area Networks (WBAN), artificial intelligence (AI), and cloud-based remote health testing. It is helpful to have an early warning system to control the infectious

* Corresponding author.
E-mail address: azana@ukm.edu.my (A.H. Mohd Aman).

https://doi.org/10.1016/j.jnca.2020.102886
Received 28 May 2020; Received in revised form 4 October 2020; Accepted 20 October 2020
Available online 2 November 2020
1084-8045/

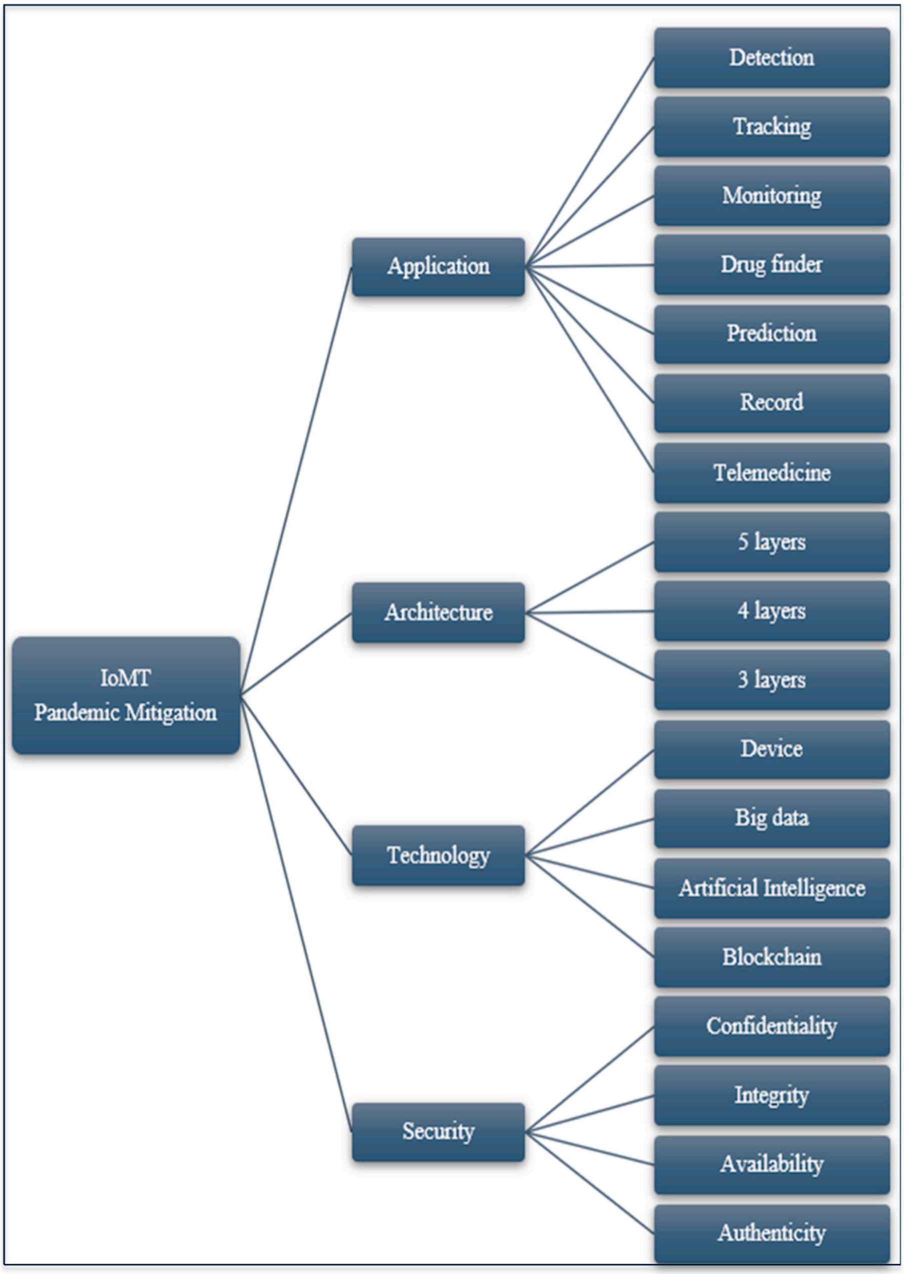

Fig. 1. Taxonomy IoMT pandemic mitigation.

diseases spread by taking advantage of the IoMT functional components like data collection, storage, transfer, and analytics. Collected sensors data by end-user hardware such as cell phones, tags, or health monitors, are transmitted to a cloud platform for decision making and analytics (Rahman et al., 2020; Al-Dhief et al., 2020; Shahidul Islam et al., 1884).

This paper provides comprehensive insights on how IoMT systems are currently being utilized within the context of COVID-19, the associated application and technology deployed, the possible architecture, and security issues concerning their usage are also discussed. The taxonomy on the insights is shown in Fig. 1.

The paper begins with an overview of the IoMT ecosystem, followed by a discussion on recent proposed IoMT architectures, the standard reference model, and possible IoMT pandemic mitigation architecture. The paper then highlights past epidemics - SARS, MERS, and EBOLA - and examines how technology, generally, and IoT, specifically, might have been applied in the past to mitigate the spread of infection. An account of IoMT-based systems and other technologies that are presently being used to mitigate COVID-19 is given in Section 5, focusing on specific countries such as Taiwan, Germany, and South Korea - these countries have managed to control the spread of the disease and limit the severity of the disease with relatively low mortality rates. A discussion on the possible security issues related to the deployment of IoMT is given in Section 6. In Section 7, we present some on-going work on the future direction and the role of IoMT with respect to big data, machine learning, and blockchain. Lastly, we conclude this paper in Section 8. Fig. 2 illustrates the flow of the paper contents.

2. The IoMT ecosystem

The medical ecosystem has evolved significantly with the rapid advancements in science, technology, and medicine, and the proliferation of smart medical devices. In addition, the advancement of communication technologies has turned various medical services into accessible virtual systems and remote distance applications. Modern

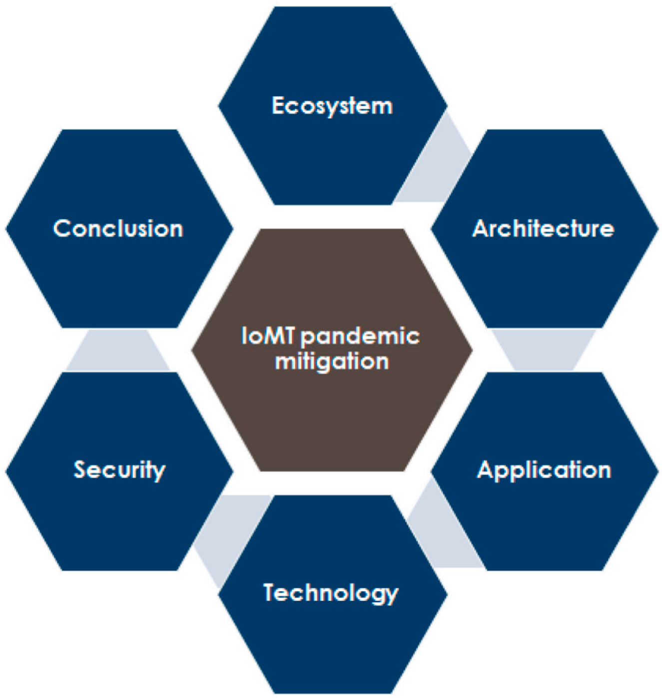

Fig. 2. Paper content flow.

implementations of the IoT into medical systems have had a tremendous impact on public life and in the healthcare industry. Researchers and industries are moving towards IoMT applications in order to provide better, cheaper, and accessible healthcare. The traditional medical ecosystem generally involves patient, doctor, medication (pharmacist), and treatment. In addition to these, IoMT medical ecosystem includes cloud data, applications (online, mobile, real-time, and non-real-time), wearable sensor devices, and security systems (Wei et al., 2020; Yaqoob et al., 2019). Fig. 3 compares a traditional medical ecosystem with a more advanced IoMT-based ecosystem.

Researchers have been proposing many interesting and implementable ideas to improve and morph the traditional medical ecosystem into an IoMT ecosystem. These enhancements apply across the board - application, architecture, technology, communication, and security components (Mohd Aman et al., 2020). The medical ecosystem framework is generally referred to the Open Systems Interconnection (OSI) model but with relevant modifications made to incorporate IoT communication and technology. The technology in IoMT refers to the hardware (firmware), middleware, and cloud platform (software). The medical ecosystem communication is the protocol used to interconnect the IoT devices, either short-range communication or long-range communication (Homei et al. 2019; Sheng et al., 2020). The medical ecosystem security involves vulnerability, attack, defense, and mitigation. The work of (Islam et al., 2015) highlights the advances in IoMT technologies, architectures, applications, and security. The security features include security requirements, threat models, attack, and risk management.

In order to support a secure IoMT system (Tseng et al., 2019), presented an approach for data verification with risk assessment. The approach defined analysis methods appropriate for selected IoT devices. Their analysis included weaknesses, attacks, and threats. Among the analyzed data are sensor data collection, data query, user registration, and management platform. In (Uddin et al., 2018), an IoMT monitoring system that preserved privacy is designed to adhere to the blockchain component. The motivation is to securely store streamed data from body area sensors. While in (Limaye, 2018) has targeted the micro-architecture design of IoMT that comprises many healthcare applications with security and data compression. Communication is an important consideration in IoMT. For example (Zhang et al., 2018), designed an IoMT system that uses Narrow Band IoT (NB-IoT) protocol (Ma et al., 2017), analyzed IoMT system with Long-Term Evolution (LTE) communication, and (Ahad et al., 2019) incorporated 5G based communication to support long range wireless communication, while the work of (Tseng et al., 2019) focused on short range wireless communication protocol, i.e., Wi-Fi and Bluetooth as part of their work on IoMT.

In IoMT cloud platform technology (Cao et al., 2020), has designed a multi-cloud computing IoMT architecture to support massive system expansion and, at the same time, support failover for storage failure recovery. The design includes a cascading manager, storage backup, resource routing, and failure recovery. In another advancement (Miao et al., 2019), highlights sensor-based smart clothing, i.e., wearable

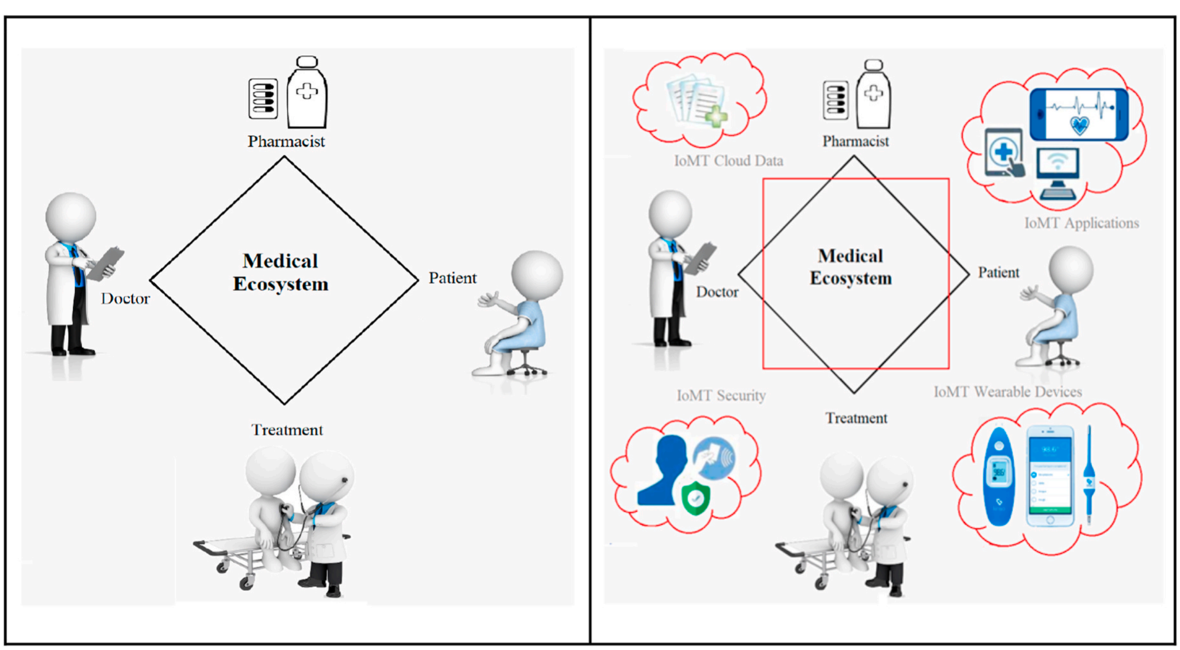

Fig. 3. Traditional versus IoMT-based medical ecosystem.

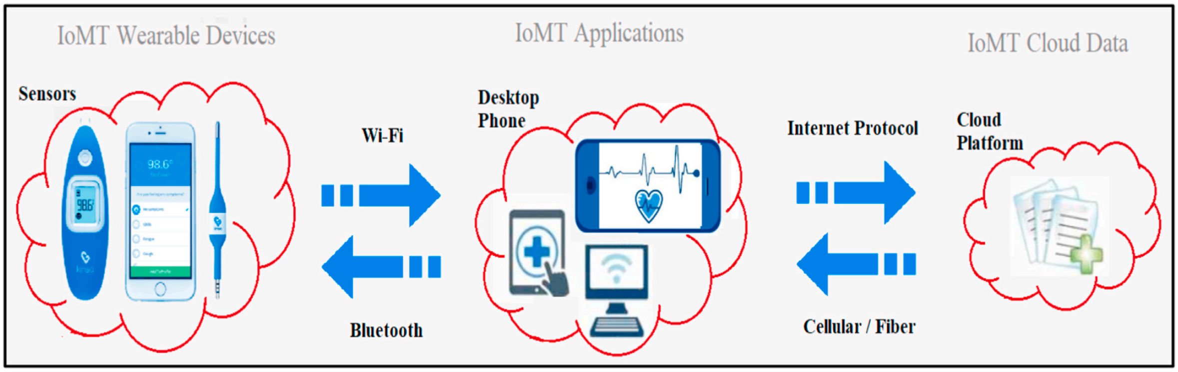

Fig. 4. IoMT communication and technology.

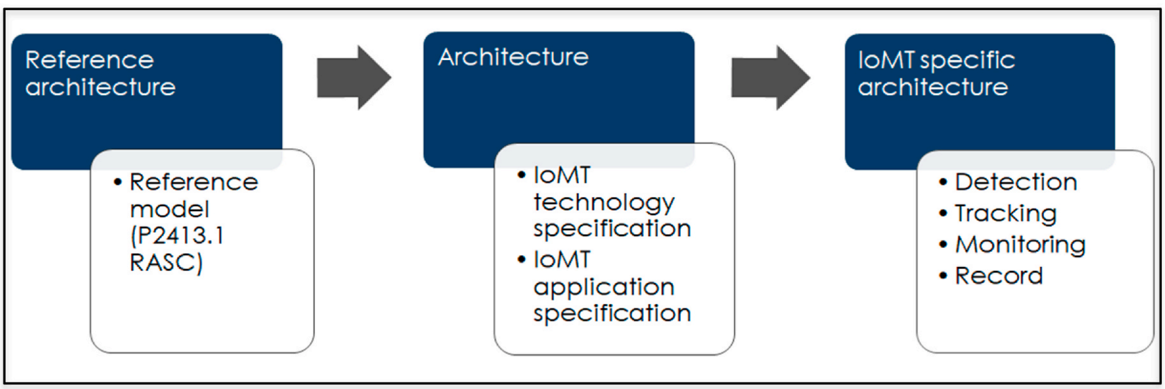

Fig. 5. IoMT framework guidance.

devices to help in remote health detection and diagnostic services. They also described a cloud-based cognitive computing and artificial intelligence robot-patient interaction. In (Uddin et al., 2018), body area sensors have been designed to operate as an IoMT continuous patient monitoring system encompassing body area sensor and sensor data provider. Fig. 4 illustrates the basic communication and technology of the IoMT ecosystem.

3. IoMT pandemic mitigation architecture

A discussion on IoMT application and technology is not complete without reference to an architecture model. Due to the many unstandardized frameworks of IoT proposed by researchers and industry, IEEE recently announced a new architectural standard for IoT (though not specific to IoMT) in Mac 2020) to promote heterogeneous interaction, system interoperability, and support further development scalability of the industry. The two new standards are P2413.1 RASC - Standard for a Reference Architecture for Smart City and P2413.2 PDIoT - Standard for

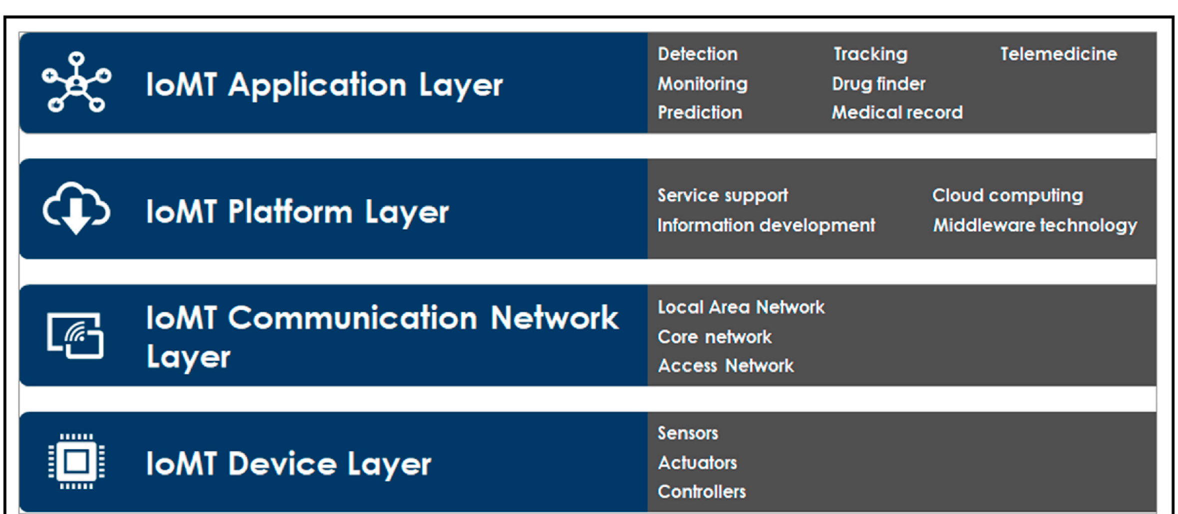

Fig. 6. IoMT pandemic specific architecture.

a Reference Architecture for Power Distribution IoT (IEEE, 2020). The standard provides guidance for the interoperability of IoT systems and is meant to unify IoT systems and minimize industry fragmentation. There are three objectives of the standard reference: i) provide a secure and interoperable IoT systems framework for multiple application domains; ii) provide a framework for assessments and comparisons of available IoT systems; and iii) provide a framework to help in accelerating design, operation, and deployment of IoT systems. Fig. 5 is the framework guidance used to develop possible IoMT specific architecture with reference to the P2413.1 RASC architecture.

The RASC standard defines a Reference Architecture with a four-layer architecture: device layer, communication network layer, IoT platform layer, and application layer. The standard includes the relation of the Intelligent Operations Center (IoC), specific to big data, cloud computing, and edge computing technologies with unified security aspects. A possible IoMT pandemic specific architecture is presented in Fig. 6.

The device layer consists of hardware such as sensors, controllers, and actuators. The RFID reader/tag, face recognition camera, fitness smartwatch, health monitoring sensors, insulin pumps, and infrared temperature sensors are among the currently used hardware. The sensors can be classified as wearable sensor devices, implantable sensor devices, and ambient sensor devices (Nanayakkara et al., 2019).

The next layer is the communication network layer. Some of the recent communication technologies used are Wireless Sensor Network (WSN), Bluetooth, ZigBee, WiFi, NB-IoT, LTE, 4G, and 5G (Ahad et al., 2019; Sengupta et al., 2019; Buurman et al., 2020; Gu et al., 2020). These are lightweight protocols that are suitable for low power devices in wireless networks such as Body Area Network (BAN) and Personal Area Network (PAN). Another important element is the aggregator, such as WiFi routers that act as gateways to provide multi-things connectivity (Noor and Hassan, 2019). A new paradigm to IoT communication is the Information-Centric Networking (ICN), the data-driven nature of the ICN enabling the data-oriented communication of IoT networks (Djama et al., 2020), where the content is the key element in the infrastructure (Nour et al., 2019; Zhang et al., 2020). ICN offers scalability, efficient routing mobility, caching strategy, and security elements to IoMT (Rathee et al., 2019; Nour et al., 2019; Zhang et al., 2020).

The IoT platform layer is another core layer that provides service support, information development, cloud computing, and middleware technology (Georgi et al., 2018). The cloud platform such as Microsoft Azure, Oracle Cloud, Amazon Web Services, Google Cloud, IBM Cloud, and Alibaba Cloud delivers services such as messaging, storage, data processing, and analytics for IoMT applications (Pace et al., 2019). The topmost layer of the IoT architecture is the application layer. This layer includes any number of devices such as monitoring system, tracking/locator system, fitness/health system, medical e-record, remote diagnose system, telemedicine, etc.

Other researchers have also proposed IoMT reference models, although not focusing specifically on IoMT specific architecture; for example (Zhang et al., 2018), presented a four-layer architecture, namely cloud computing layer, edge computing layer, base station layer, and sensing layer. Similarly (Ma et al., 2017), presented an IoMT system architecture comprising of a four-layered architecture - perception layer, transport layer, cloud service layer, and cloud-to-end fusion (Din et al., 2018). identified health system as among IoT based smart cities application concluded the architecture layer as sensing, network, cloud computing, and application layer.

While (Sengupta et al., 2019) generalized the IoT architecture as perception layer, network layer, processing layer, and application layer. Focusing on the component interconnection between IPv6 and the physical network (Liu et al., 2018) designed a simplified protocol message format instead of using packet format conversion. This was developed to satisfy IoMT functional requirements using a five-layer architecture - sensing/execution layer, communication auxiliary layer, network transmission layer, data integration layer, and application service layer. Alternatively (Xu et al., 2019), has introduced a four-layer system architecture based on IoT - application layer, network layer, analysis layer, and sensing layer. The objective was to improve transmission for remote diagnose and treatment that require data processing and data visualization for three-dimensional images and, at the same time, provide data transmission security.

An IoMT architecture with security specification may be subsequently defined by augmenting specific medical-centric elements to the Application Layer (Noor and Hassan, 2019). Such components may include medical-wearable IoT systems, e-health applications, ambient sensors, remote diagnostics, and other non-wearable medical systems. Based on this proposed architecture, security aspects of the IoMT system would still be preserved and enforced since the Application Support sub-layer, as well as the Network and Perception Layers have been tightly integrated with security elements within the framework. Thus, any new IoMT system built conforming to this security architecture would have multi-layer defense-in-depth mechanisms in-placed by default.

Table 1 summarizes the architecture layer analysis, while Fig. 7 shows the percentage of the layer analysis. The four-layer architecture is the most preferred framework, as it contains classification of application, virtual platform, network communication, and physical aspects of IoT.

Table 1
Summary of architecture layer analysis.

Architecture layer	5 layers	4 layers	3 layers	Ratio
Application	Liu et al. (2018)	Xu et al. (2019); Din et al., 2018; Sengupta et al. (2019); IEEE, 2020	Noor and Hassan, 2019	19%
Cloud computing		Zhang et al. (2018); Din et al., 2018		6%
Cloud-to-end-fusion		Ma et al. (2017)		3%
Cloud service		Ma et al. (2017)		3%
Platform		IEEE, 2020		3%
Processing		Sengupta et al. (2019)		3%
Data integration	Liu et al. (2018)			3%
Edge computing		Zhang et al. (2018)		3%
Transport		Ma et al. (2017)		3%
Network	Liu et al. (2018)	Xu et al. (2019); Din et al., 2018; Sengupta et al. (2019)	Noor and Hassan, 2019	16%
Analysis		Xu et al. (2019)		3%
Base station		Zhang et al. (2018)		3%
Communication	Liu et al. (2018)	IEEE, 2020		6%
Perception		Ma et al. (2017); Sengupta et al. (2019)	Noor and Hassan, 2019	9%
Sensing	Liu et al. (2018)	Xu et al. (2019); Din et al., 2018; Zhang et al. (2018)		13%
Device		IEEE, 2020		3%

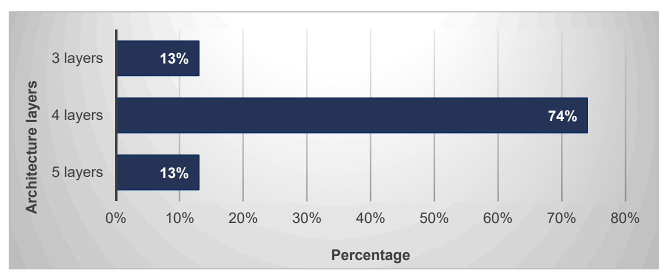

Fig. 7. Architecture layer analysis percentage.

4. Past epidemics and technology utilized

A system that integrates IoMT architecture and technology comprises of RFID, WBAN, and cloud services is able to provide a reliable healthcare monitoring and early-stage detection system for pandemic diseases (Sareen et al., 2016). But in such circumstances, the system would have to be handled by highly trained professionals because of the highly infectious nature of these viruses. The system captures real-time close immediacy contacts and records health data to control the epidemic spreading. This type of system is used in COVID-19 pandemic mitigation. However, during Severe Acute Respiratory Syndrome (SARS-CoV), Middle East Respiratory Syndrome Coronavirus (MERS-CoV), and Ebola epidemic, the IoT technology had not yet matured; hence it could be the reason why few approaches were made to use it to combat the epidemics.

4.1. SARS-CoV (Asia)

In 2002, the SARS-CoV was identified in the city of Guangdong of the Chinese province through traces of human infections, yet the source of this virus was never clear (CDC, 2003). SARS-CoV was recognized as the first distinct strain of coronavirus in 2003. The disease, with the symptoms similar to the influenza was spread across 26 countries, infecting more than 7000 people and causing around 800 deaths.

One of the few IoT applications used for SARS was by the Singapore government. This was to implement home quarantine for suspected infected people with SARS through the use of online cameras (WHO, 2006). Electronic cameras were installed at the houses of quarantined people, for broken quarantine cases, written warnings together with electronic wrist tags would be given. The authorities would be notified if the tag is broken or when the person leaves the house as the tag is linked to a dedicated telephone line.

Geographic information systems provided valuable information to track infected cases and analyze the new disease source. The GIS systems were used in the SARS-CoV epidemic in 2002 (Boulos, 2004; Braden et al., 2013) as well as seasonal influenza in 2020 (Control and Prevention, 2020).

4.2. MERS-CoV (middle east)

In 2012, people exhibiting cough, shortness of breath, diarrhea, and fever were identified as MERS-CoV victims. The discovery of a new virus took quite a few months, the syndrome was identified first in Saudi Arabia, the evidence pointed to dromedary camels as a possible source of infection, but this was never officially confirmed (CDC, 2015). Among the earlier cases were reported from Jordan, Qatar, Saudi Arabia, and the United Arab Emirates. Like SARS, the new virus causes patients to experience kidney failure and severe pneumonia (Momattin et al., 2013).

Revealing accurate real-time information such as the list of hospitals affected by MERS-CoV is important as it prevents more infections and minimized the number of positive cases (Noh et al., 2020). (Sandhu et al., 2016) suggested that to control the epidemic in its early stages, a system was needed to deliver symptoms early diagnose, separation of population at risk using geographic positioning system, and secure the personal information of positive cases to avoid mass panic paranoid.

4.3. Ebola epidemic (West Africa)

The Ebola Virus Disease (EVD) outbreak was reported in March 2014 by the World Health Organization (WHO). The first case was detected near the village of Meliandou, in Guinea (Baize et al., 2014; Briand et al., 2014). The virus quickly spread across other four other countries as the surrounding area was one of the most populated areas in West Africa. By August 2014, WHO announced this outbreak as a “Public health emergency of international concern” (Team, 2014). In September 2014, 4507 cases of EVD and 2296 deaths from this disease were confirmed in five countries, including Guinea, Nigeria, West Africa, Sierra Leone, and Liberia (Organization, 2014a; 2014b; 2014c). Later, the number of infected cases increased to 28,652, where a total number of 11,325 of them died (Bell, 2016; Poletto et al., 2014). In 2018, a new EVD epidemic was reported in Mbandaka, Democratic Republic of the Congo (Gostin, 2018; Green, 2017; Leggiadro, 2019; Telionis et al., 2020).

IT and communication technologies have penetrated every domain of human life, especially in public health. The mobile phone usage is widespread in some African countries; as an example, SMS service is used in Madagascar as a reporting method for surveillance systems (Aliya, 2014; Louis, 2012; Randrianasolo et al., 2010). Furthermore, a large number of Ugandan health system workers collect health data using smart gadgets such as PDAs (Consulting, 2009). There are many confirmed reports of the use of IT technologies such as smartphones, communication networks, artificial intelligence, contact tracking, GIS, and social media during the Ebola outbreak in Africa. In this section, various information technology approaches used to control EVD outbreak are summarized and discussed. Boulos and Geraghty (2020) conducted research to describe a range of practical mobile GIS and applications for tracking infected cases in time of disease outbreak. WorldPop mapped population distributions and mobile phone flow map in African countries to assist in controlling Ebola virus outbreak in 2014 (WorldPop, 2014).

Fan (Fan et al., 2020) investigated the Spatio-temporal pattern of EVD in most infected West Africa countries to find a spatial association between these patterns and other geographical factors. According to this study, the prior studies (Chowell and Nishiura, 2015; D'Silva and Eisenberg, 2015; Kramer et al., 2016; Shaman et al., 2014) proved that the geographical location of the infected people have a direct impact on spreading of Ebola virus, and the majority of these researches claimed that GISs were used to monitor and track infectious diseases.

Mobile-based digital management is another type of using information technology to support controlling and managing disease outbreaks. In 2020, Yavlinsky et al. (2020) conducted a research on mobile-based case detection in disease outbreaks and management system, which leveraged a systematic review conducted by Tom-Aba et al. (2018). They analyzed various management systems such as Surveillance and Outbreak Response Management and Analysis System (SORMAS) (Fähnrich et al., 2015), CommCare (“CommCare for Ebola response,” 2019), and AfyaData (Karimuribo et al., 2017). All these methods are analyzed and evaluated based on criteria such as contact tracking, case management, surveillance, and lab results. Based on analysis results, SORMAS, which is an open-source system that performs real-time analysis via a web application interface, satisfies all discussed criteria. The 2015 version of SORMAS was designed for Ebola virus outbreak control with the cooperation of healthcare centers in Nigeria.

5. IoMT application and technology for COVID-19

The scalability of IoT supports the monitoring of a large number of patients from their homes or hospitals. Their biometric measurements, such as blood pressure and heartbeat, may be transmitted to the cloud for analysis without exposing healthcare workers to the infection (Ting et al., 2020). IoT has already been used in identifying and tracking the origin of an outbreak and ensuring the quarantine of potentially infected patients (Song et al., 2020).

One study of using IoT to detect a fever was done by (Zhu et al., 2019), who proposed an inexpensive IoT system that automatically uploaded resulting data using wireless Bluetooth communication to an Android-based smartphone to a global network. Hence the test results are available immediately, anywhere in the world. Such an IoT system is a very crucial tool for medical practitioners in order to tackle infectious diseases.

An earlier study by (Massaro et al., 2019) used mobile phone data to trace the spread of dengue virus in Singapore during 2013 and 2014 with details of short distances and periods. Therefore, overlaying GIS on IoT mobile data from any infected patient may lead to two things: assist epidemiologists in their search for patient zero, and help identify anyone who has had contact with an infected patient(s) and is at a high risk of being infected. In another study (Peeri et al., 2020), compared the epidemics of the three coronaviruses and concluded that there were no frequent outbreaks found from SARS and MERS, and the applications of IoMT may lessen the severity of COVID-19 in reducing and controlling the incidence of infections among members of the general public.

5.1. COVID-19 in Taiwan

Within days of the first COVID-19 case detected in Taiwan on January 21, government officials decided on several initiatives to impede the spread of the disease, especially from those who had returned from China after the Lunar New Year break (Tsai, 2020). These measures include case identification, containment, and deployment of new technologies.

Digital Surveillance: Leveraging on big data analytics, generation of real-time alerts, QR scans, travel history information, and other resources, Taiwanese officials could identify and classify individuals into several distinct categories of risk (Wang et al., 2020). Those identified as high risk were told to quarantine at home and to remain so during the incubation period. By early February 2020, a cellphone-based digital system had been developed and deployed to monitor and track those quarantined individuals (Hui, 2020). The system, a collaborative effort between five major telecommunications companies and the Taiwanese government, was able to track quarantined individuals by triangulating the location of their phones relative to nearby cell towers. If the cell phone of an individual was turned off or if a person was found to have broken quarantine, an alert would be triggered within 15 min (Lee, 2020). Front-line personnel (usually Police officers) would then be deployed, typically assisted by accessing cloud-based databases (known as M-Police system) to locate these individuals, and hefty fines would be imposed. Although privacy concerns were abounded, a recent poll indicates the majority (84%) of Taiwanese people firmly support the government tactics to impede the spread of the disease, which has resulted in a significantly fewer number of cases compared to neighboring China (Taiwanese Public Opinion Foundation, 2020).

Wearable IoMT: Taiwan's iWEECARE company developed a small wearable IoMT device, called Temp Pal, that is able to detect abnormal temperatures and send corresponding alerts (Koh, 2020). The Temp Pal system consists of a stamp-sized soft patch, weighing 3 g with a battery life of 36 h per charge, and is able to transmit continuous temperature data via Bluetooth Low Energy to a mobile app and its cloud dashboard. The device gathers data wirelessly through its specialized BLE/Wi-Fi gateways, which collect patients' temperatures via their Temp Pal smart patches attached to their bodies. The IoMT system, used by both hospitals and self-quarantined individuals, allows real-time monitoring while reducing the incidence of direct contact between patients and caregivers, thus mitigating the spread of disease. According to Taiwan's Cheng Hsin Hospital where the technology is deployed (Koh, 2020), the cloud-based temperature monitor system has saved medical personnel time, reduced recording errors, decreased consumption of personal protective equipment (PPE), and most importantly, lowered the risk of infection to front-line personnel.

AI-powered IoMT: An AI-powered IoMT detection system has been deployed at Taiwan's Yonghe Cardinal Tien Hospital (Microsoft, 2020). The 2-in-1 smart detector, developed jointly between Microsoft Taiwan Azure and local IoT providers, leveraged on AI, intelligent IoT edge system, and cloud services to continuously scan people, in real-time, as they enter the hospital lobby. The system detects body temperature via infrared scans and also determines if the person is wearing a protective face mask using AI technology. First-line hospital staff is alerted immediately when either abnormal temperature or the absence of protective mask is detected on any individual entering the hospital. This system allows for a higher degree of protection for hospital staff and patients while easing the burden of valuable manpower for continuous monitoring.

5.2. COVID-19 in South Korea

Among the countries highly affected by COVID-19 from the initial stages of this pandemic is South Korea. In January 2020, the first case was reported, a female from Wuhan city who had stopped over in the South Korean airport (Her, 2020). At the time, the situation was still under control with slightly more than 30 cases, and concerns on the contagiousness of COVID-19 initiated considerations to strengthen border control as well as devise suitable disinfection protocols. A turning point that causes a massive epidemic in South Korea occurred in February where a "superspreader" attended the Shincheonji Church in Daegu, Seoul. Other worshippers at the church were subsequently infected — a single case that has since infected more than 6000 people (Moon, 2020).

South Korea's approach to flattening the curve without imposing a total lockdown has been lauded by many countries around the world. The concept of flattening the curve is to reduce the number of new cases so as not to overwhelm the capacity and capability of the healthcare system while reducing the spread of the virus (Leite et al., 2019). A total lockdown would be detrimental to the country's economy and may result in recession and unemployment that would be hard to recover (Rogoff, 2020). South Korea has managed to curb the transmission of the virus by integrating and adopting multiple strategies based on discussions amongst health-care professionals, technical committees, and government agencies. Their approach, known as the 3 T, stands for Trace, Test, and Treat (MOHW.kr, 2020, Leite et al., 2019). Although IoMT is primarily used in their 'Trace' strategy, the other two strategies (Test and Treat) are described briefly as well for the sake of clarity and completeness.

Trace: This strategy details measures pertaining to special entry procedures and begins with a complete health questionnaire to solicit information from individuals who have had previous travels or stopovers in countries with a large number of confirmed COVID-19 cases. Affected travelers are required to undergo compulsory self-quarantine for 14 days (Chinazzi et al., 2020) before any test of swab is issued. Individuals were reminded to practice social distancing (Shim et al., 2020], wear masks, and practice good personal hygiene. Each new arriving individual was also required to download a self-diagnosis app on his/her smartphone. The app was then used to conduct digital tracing on the individual (Ferretti et al., 2020). The contact tracing mechanism consists of 4 phases, namely initialization, sensing, reporting, and tracing. The app keeps all movement records of the self-quarantined individuals. Once the individual is a confirmed COVID-19 case, all information of his movement would be downloaded by the Health Authority to trace his/her contacts. Telephone calls were made to monitor individuals who did not install the app. Calls were made by the Health Authority on a daily basis for 14 days, and in addition to this, a 1339 Call center was made available to call public health centers. The call center gives advice on 'safe' hospitals and is able to handle a maximum of 70, 000 calls daily manned by healthcare consultants. Information updates on confirmed cases were disseminated quickly and transparently to the public so that they are aware of the location of infected premises. Briefings were conducted on a twice-daily basis, and the Central of Disease Management (CDM) Headquarters and Central Disease Control (CDC) Headquarters have held 120 sessions since January 20, 2020.

Test: A triage room was established to perform epidemiological investigation on confirmed cases, overseas epidemic control, and disinfection work for each respective locality. In addition, swab testing was reduced to just 10 min through a drive-through process. With this drive-through approach, the cost of Personal Protective Equipment (PPE) was further reduced since one does not need to change to another PPE set after a swab test is made. Hence, the combined capacity of

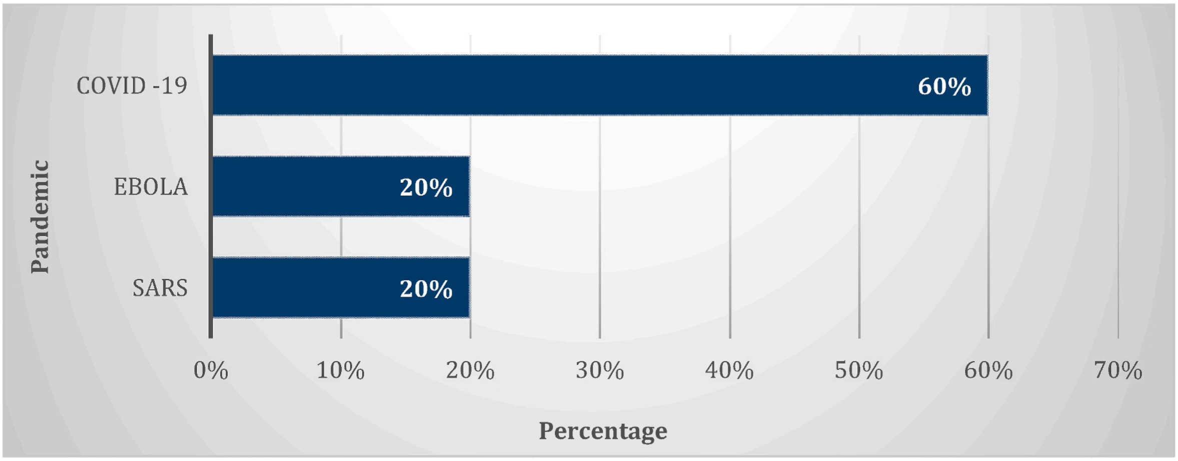

Fig. 8. Pandemic and its applications percentage.

testing laboratories across South Korea was ramped up from a capacity of 10,000 to 20,000 tests daily.

Treat: In response to COVID-19, the South Korean government established a National-Designed Isolation Unit (NDIU) - a hospital ward, funded by the government that is on standby to receive patients infected with the disease. The ward is well equipped with a negative pressure system and is staffed by well-trained professionals. Residential treatment centers were also established to admit patients with mild symptoms or those asymptomatic to COVID-19 - to enable them to recover naturally or with symptomatic treatments alone. Hence, patients that require priority care can be forwarded to the specialized hospitals.

5.3. COVID-19 in Germany

Germany is among the most advanced countries in technology and the most innovative country (Jamrisko, 2020), built a think-tank project with the aim of accelerating the digitization of healthcare in Germany so as to mitigate COVID-19. The health innovation hub issued a list of telemedicine services (comprising reimbursement policy, associated costs, and functionalities) that is easily accessible by medical staff without the need to have significant technical and/or hardware investment.

Germany launched a smartwatch application to detect infections and mitigate the spread of COVID-19. The application collects vital signs (such as body temperature, heart rate, and sleeping time) from patients wearing the smartwatch in order to predict if they are infected with the virus. This prediction, with other collected data, is accessed by health authorities through an online map to assess the prevalence of infections (Busvine 2020). In addition, a German startup, DOCYET, launched an application that predicts if a person has the symptoms of a typical SARS-CoV-2 infection. The app is called Corona-Bot, and is frequently updated based on the latest scientific published studies and data provided by scientific institutions.

Bosch has also developed a rapid diagnostic device that is able to confirm COVID-19 infection in a matter of hours (as opposed to days for results). The device enables quick identification and isolation of infected individuals, thereby reducing the spread of the disease. Another feature of this device is that it may also detect other respiratory diseases such as influenza A and B. This device is expected to be available in Germany by April 2020 (Bosch, 2020). Also, Germany has enforced the use of passenger locator cards (US embassy Consultant, 2020). This card allows for rapid action to collect the passenger's contact information. Accordingly, WHO is encouraging the use of this card in order to limit the spread of diseases while onboarding aircraft and for the subsequent need for contact tracing (WHO, 2020). Professor Jörg Debatin, head of the health innovation hub in Germany, stated that "We have not gone far enough with the digital agenda in Germany to respond fully to the COVID-19 crisis and many innovations that could help are planned but have not yet implemented (Olesch, 2020).

Table 2
Pandemic technology and application.

Pandemic	Application	Device	Objective
SARS-CoV (WHO, 2006; Boulos, 2004; Braden et al., 2013)	Online camera	Camera	
	Electronic wrist tag	Tag	
	Geographic information system	Mobile phone	
Ebola (WHO, 2014a, 2014b, 2014c; Aliya, 2014; Louis, 2012; Randrianasolo et al., 2010; Fähnrich et al., 2015; Tom-Aba et al., 2018; Yavlinsky et al., 2020)	Surveillance systems	Mobile phone, PDA	
	Geographic information system	Smartphone	
	Mobile-based digital management	Mobile phone	
COVID-19 (WHO, 2020; Wang et al., 2020; Hui, 2020; Lee, 2020; Koh, 2020; Microsoft, 2020; Leite et al., 2019; Mohw.kr, 2020; Ferretti et al., 2020; Busvine, 2020; Draper, 2020; Bosch, 2020)	Tracking application	Cell phone	• Virus predictive trend • Risk of mortality prediction • Drugs candidate finder • Genomes systematic classification • Priority prediction
	Temperature alert application	Wearable device, mobile phone	
	2-in-1 smart detector system	Infrared scan, camera	
	Self-diagnosis application	Smartphone	
	Digital tracing application	Smartphone	
	Telemedicine service	Smartphone	
	Smartwatch application	Smartwatch	
	Rapid diagnostic device	Disease detector	
	Passenger locator	Locator card	

Fig. 8 shows the percentage of applications used in mitigating SARS, Ebola, and COVID-19. The advancement of IoT technology has contributed to the number of applications developed. Table 2 summarizes the analysis of the application and technology used.

6. Artificial intelligence and big data technology in IoMT

The high fatality rate of COVID-19 has caused an imbalance in the public health system. Hence it has become one of the main goals in recent technology research to control the outbreak and, at the same time, reduce the transmission of the pandemic (Lai et al., 2020). Public health and infection control measures are urgently needed to reduce the overall spread of the virus in order to reduce the damage associated with COVID-19. Experience from the early phase of COVID-19 pneumonia has demonstrated that travel experience, rather than chest radiography, is of vital significance for early diagnosis and insulation of cases (Lai et al., 2020). Therefore, limiting human-to-human transmission is essential in order to reduce secondary infections among close contacts and healthcare workers and to prevent further global spread.

Every effort is being made to slow the spread of disease in order to provide time for better preparation of healthcare systems and the general public, to better characterize COVID-19 to guide public health recommendations and to develop timely diagnostics, therapeutics, and vaccines. Focus on maintaining significant social distancing of the entire population, and thereby halting the spread of the disease is crucial. Some use Artificial Intelligence (AI) to simulate human intelligence in machines programmed to think like human beings. An AI system displays characteristics consistent with a human mind, such as learning and problem-solving. Method such as mathematical computational complexity theory (such as non-deterministic polynomial time) focused on classifying computational problems by linking classes and resources to each other like an algorithm (Hosseini et al., 2020). An algorithm can be of 1) an approximation technique that looks for a solution that is at most an optimum one or, 2) randomization technique, a faster average running time and allow the algorithm to fail with a small probability such as genetic algorithms, or 3) restriction technique by reducing the size of inputs or 4) parameterization where certain input parameters are fixed, or 5) heuristic technique (metaheuristic approaches are frequently used).

According to (Hosseini et al., 2020), there is a need for an effective computational complexity theory, such as an optimization algorithm that can control the outbreak and, at the same time, reduce the transmission of the pandemic (Hosseini et al., 2020). developed an algorithm specifically for COVID-19 to cover nearly all feasible regions of optimization problems by modeling the mechanism of coronavirus dissemination in many countries across the globe. The model reduces the number of contaminated COVID-19 countries and thereby slows down the spread of the epidemic. In addition, the model complies with three hypotheses that are aimed at solving the optimization problem by using the most efficient distribution variables. It addresses a significant question: how can policymakers and health institutions be able to bring people back to their normal lives in the age of the dissemination of COVID-19?

Data mining in IoMT may play an effective role in building predictive models as presently, there is no accurate and specific method to forecast the impact of diseases such as COVID-19 (Cascella et al., 2020). Data that is generated by IoT devices are streaming data that continues to grow in volume and velocity and is considered by a few researchers as pure big data (Marjani et al., 2017). Big data analytics may be viewed as an independent study of health care statistical data patterns to build predictive models. As part of AI, Machine Learning (ML) is an analytical methodology that can simulate an occurrence with fair precision based on the knowledge and learning process. In the meantime, a fast number of ML models have been developed to replicate the cases of COVID-19 (Mohammed et al., 2020).

In recent years, smart, innovative frameworks have emerged, fusing IoT and big data analytics for the healthcare industry (Saheb et al., 2019). ML and big data mining have already been used in the past for disease prediction and analysis (Dimitrov, 2016; Hameed et al., 2017; Vinitha et al., 2018). In addition, the development of new pharmaceutical drugs and vaccines has been made possible using various applications of ML algorithms - for example, Google has begun work on pharmaceutical drug development using ML methods and techniques (Pramanik et al., 2017). Work by Dimitrov (2016) showed a unified classification and association rule mining algorithm to classify the rules underlying the modification of non-pandemic sequences to pandemics in influenza pandemic databases. The researchers proposed that the derived rules could contribute to the construction of an effective expertise framework for forecasting influenza pandemics.

Additionally (Mohammed et al., 2020), suggested an insightful ML approach to assist health institutions in the application of the COVID-19 diagnostic device. Benchmarking and testing diagnostic models for COVID-19 is not a straightforward process. Multiple criteria are required to be assessed, and some of the criteria are in conflict with each other. Hence a decision matrix that combines assessment parameters and diagnostic models for COVID-19 to obtain multi-criteria decision-making with respect to the assessment criteria is needed. The criteria of the diagnostic model are not entirely addressed by the testing approaches. In addition, these methods are constrained in effectiveness since they require the estimation of all arguments. They are, therefore, unable to equate and match two classifiers because of the inability of these approaches to rate various classifiers on the basis of their results. The benchmarking and assessment process in the COVID-19 classification systems is known to be a multi-objective/criteria problem. The goal is to provide an integrated framework for the assessment and benchmarking of various COVID-19 diagnostic classifiers. This motivates the development of unified classifiers within a single system, covering all the efficiency dimensions of the assessment of the COVID-19 classifier models. The technique developed is used as an assistance mechanism to help decision-makers in the medical and health association determine which of the best classification schemes can be used to diagnose COVID-19 by comparing various classification models.

In a recent study (Jia et al., 2020), utilized data from 2003 SARS to generate three mathematical models, namely the Logistic model, Bertalanffy model, and Gompertz model, in order to develop a predictive trend on the virus. The three models were then used to fit and study the epidemic trend of COVID-19 in Wuhan, mainland China and non-Hubei areas. Based on this work, the researchers predicted the total number of infections and deaths that would occur in Wuhan and China mainland and non-Hubei areas. In addition, they predicted the time that the pandemic will end in China, which is late in April 2020. Based on their prediction and at the time of writing, their prediction has shown to have some degree of accuracy.

In another study, a machine learning tool was developed to raise awareness of handwashing in the time of COVID-19 pandemic (Pandey et al., 2020). This is where health data of 2799 patients with COVID-19 was screened, and the prognostic prediction model was built based on the XGBoost machine learning algorithm and then tested against 29 patients to predict criticality in patients with severe COVID-19 infection. The authors have stated that their model is capable of well predicting the risk of mortality and that it provides a clinical pathway for the recognition of critical cases from serious cases, thereby reducing the number of deaths (Pandey et al., 2020). Moreover, since there is no biomarker to distinguish those who will develop severe cases from COVID-19, the need for predicting critical cases arises. In another study (Yan et al., 2020), a mathematical simulation method based on machine learning was proposed to recognize the most important biomarkers of patient survival. This helps to give priority to those patients in giving treatment and saving more lives.

(Arun and Neelakanta Iyer, 2020) provides an overview of the spread of COVID19 disease and estimates the severity of the pandemic, the survival rate and the fatality rate using known machine learning methods as well as mathematical simulation techniques such as Rough Set-Support Vector Machine, Bayesian Ridge and Polynomial Regression, SIR Model and Recurrent Neural Network. The goal is to determine the relationship between the dependent variable and the independent variable. The model is described as susceptible (the individual has not contracted the disease, but can be infected through transmission from infected individuals, infected (the individual has contracted the disease) and recovered/deceased (the disease can lead to either of two fates: either the person survives, while losing the immune system). The study

Table 3
IoMT artificial intelligence and big data.

Reference	Scope	Predictive Model	Data Mining & Analytics	Decision Making	Systematic Classification
Dimitrov (2016)	Healthcare domain	Yes	Yes		
Vinitha et al. (2018)	Disease domain	Yes		Yes	
Saheeb et al., 2019	Healthcare domain	Yes	Yes		
Cascella et al. (2020)	COVID-19 disease domain	Yes	Yes		
Jia et al. (2020)	COVID-19 disease domain	Yes			
Pandey et al. (2020)	COVID-19 disease domain	Yes			
Allam and Jones, 2020	COVID-19 disease domain		Yes		
Paraguassu et al. (2020)	Coronavirus and COVID-19 disease domain		Yes		Yes
Inn (2020)	COVID-19 disease domain		Yes		
Pramanik et al., 2017	Healthcare domain			Yes	
Yan et al. (2020)	COVID-19 disease domain			Yes	
Vaishya et al. (2020)	COVID-19 disease domain			Yes	
Ratio		35%	35%	24%	6%

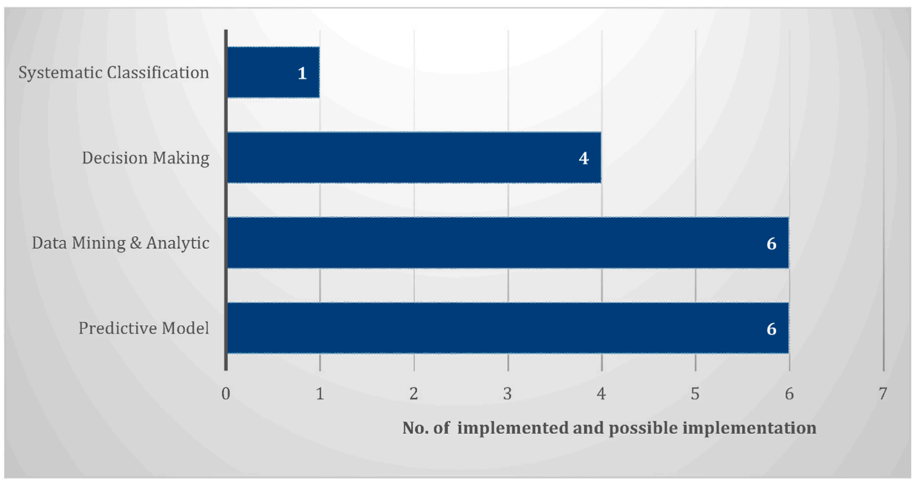

Fig. 9. Artificial intelligence and big data number statistic.

was based on the data collection provided by the Johns Hopkins Corona Virus Resource Center. The Recurrent Neural Network model was the most effective of the machine learning methods used in the experiment. The findings are helpful in forecasting and preventing the outbreak of any epidemics or pandemics in every country or the globe.

Advanced machine learning methods have been utilized in a systematic classification of COVID-19 genomes, CRISPR-based COVID-19 detection assay, and finding drug candidates against COVID-19. In

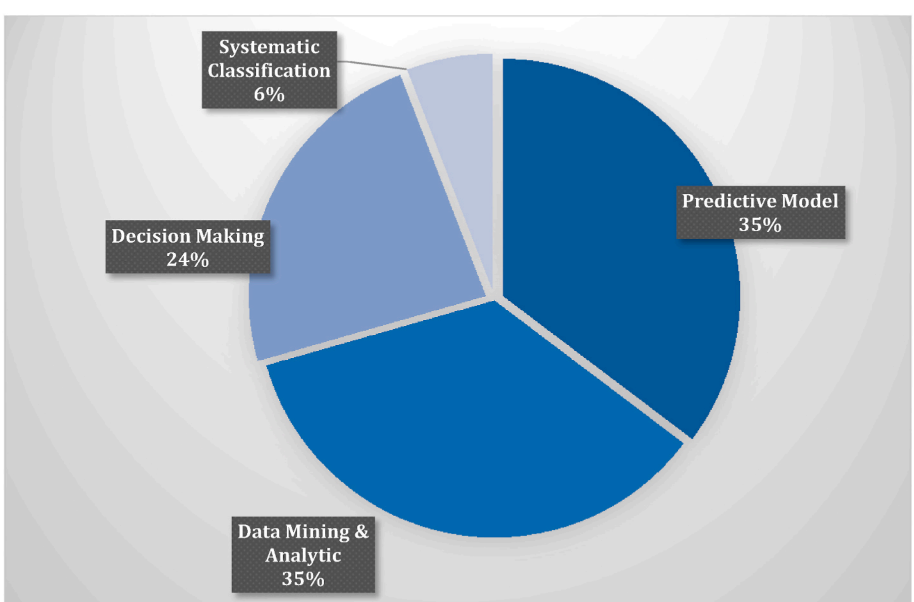

Fig. 10. Artificial intelligence and big data analysis percentage.

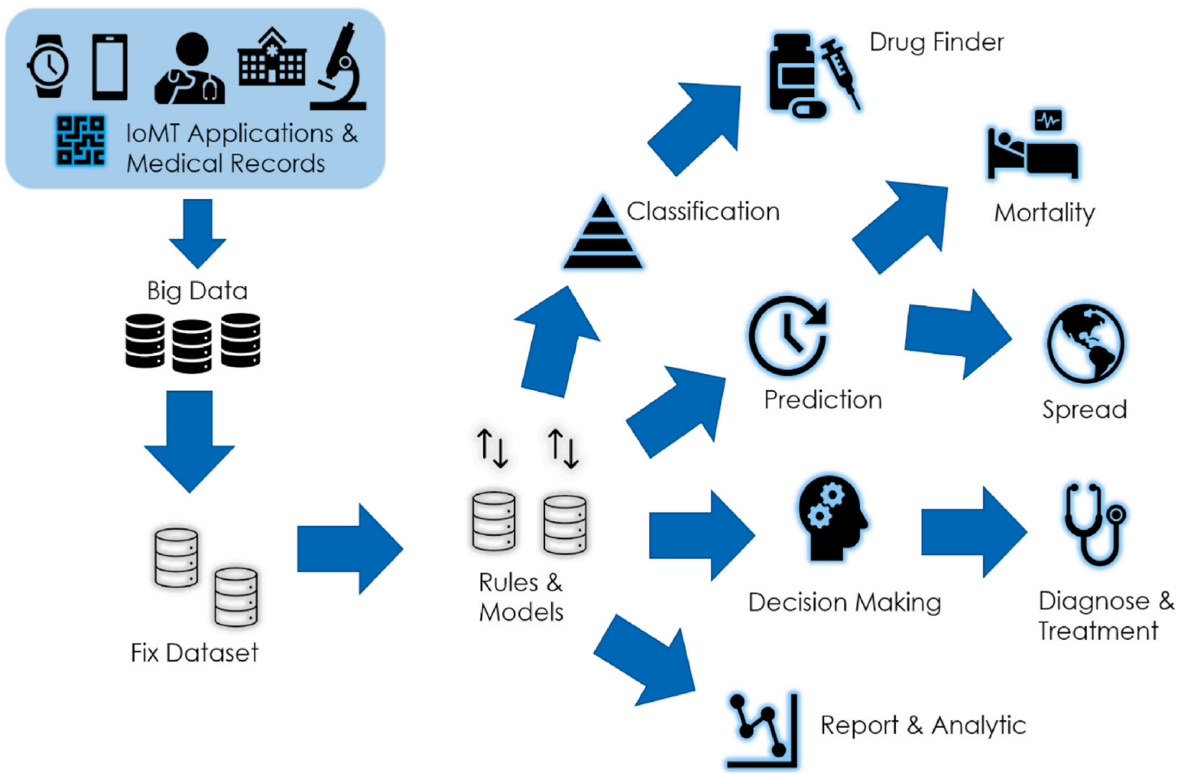

Fig. 11. IoMT, big data and artificial intelligence for COVID-19 mitigation.

addition, recent studies suggest that the internet of things (IoT) and related technologies such as AI, Big data analytics, next-generation 5G communication can play a vital role in preventing the spread of infectious diseases such as COVID-19. This facilitates simultaneously the data recording, patient health tracking, data analytics, and alerting (Paraguassu et al., 2020; Peeri et al., 2020).

The application of AI in China and South Korea has been demonstrated during the continuing COVID-19 outbreak. Highlights on the use of medical IoT towards COVID 19 is the application of infrared cameras and the face detection system capable of identifying any person at high temperature. In order to reduce the possible risk of the COVID-19 in exposure to authority when conducting direct body temperature measurements, China built robots fitted with AI. This technology is driven by 5G and fitted with five high-resolution cameras and infrared thermometers. The robots are capable of measuring 10 person's body temperature at the same time within a distance of 5 m.

WHO has also recognized that China has successfully used big data and AI during the COVID-19 pandemic (Inn, 2020). Noticeably, there is a desperate need for decision-making tools to control this epidemic to support health organizations to make effective decisions in order to prevent its dissemination. A result-driven technology was developed for accurately testing, analyzing, and monitoring of existing patients, and forecasting new cases. These technologies have utilized data of reported, recovered, and dead cases (Vaishya et al., 2020).

Table 3 summarizes the discussed IoMT Artificial Intelligence and big data technology and the functionality scopes. Fig. 9 statistically shows the number of implemented and possible implementation of the analyzed IoMT Artificial Intelligence and big data technology. While Fig. 10 illustrates the percentage ratio for the four function scopes. The predictive model and data analytics are the most used functions, followed by decision making. The graphical abstract of IoMT applications and technologies for COVID-19 mitigation is shown in Fig. 11.

It is clear that big health data analytics can be used to predict unseen patterns and hidden information about pandemics. Moreover, medical IoT can be considered as another face of the health industry, and in some cases, IoMT with big data analytics can perform better than health organizations in diagnosing, treating, and predicting such unknown diseases. However, to obtain a potential technology, by combining big data analytics and the medical internet of things, there is an immediate need to move towards standardizing the decentralized data (Allam and Jones, 2020). Owing to the availability of data in terms of form and length, the values of the various models used may be modified (Mohammed et al., 2020). In realistic words, the large number of ML learning models have contributed to a big challenge for the management teams of medical institutions to choose the most suitable model they consider to be the key problem of this research.

Moreover, the incorrect selection of a diagnosis model for COVID-19 can be expensive for medical organizations, particularly at a time when there is a tremendous need for a more reliable and rapid diagnosis model. A flexible full coverage approach helps them to test and compare a range of COVID-19 diagnostic models and settle on the selection of a model that fits the needs of a health institution and reduces time and money by using a rigorous framework for the selection of ML models. A scalable approach that can be extended to benchmarking diagnostic models based on radiology laboratory data such as CT images, which will basically allow the medical institution administration to choose the most appropriate COVID-19 diagnostic model (Mohammed et al., 2020).

Other difficulty in COVID-19 ML research is the dataset itself. As the data is rising on a regular basis and that the number of cases grows increasing exponentially (Arun and Neelakanta Iyer, 2020; Mohammed et al., 2020). As several research include the application of a mix of neural networks and conventional machine learning techniques, issues such as diagnostic models, benchmark standard, updated requirement, and variables are among significant concerns (Mohammed et al., 2020). The multiform of COVID-19 diagnostic models should be tested and benchmarked using the standard trusted approach in subsequent experiments. The requirements must be UpToDate for the assessment and benchmarking process. The ML applications of any new variables must have a fixed recent dataset.

While improving IoMT, AI, and Big Data, internet communication

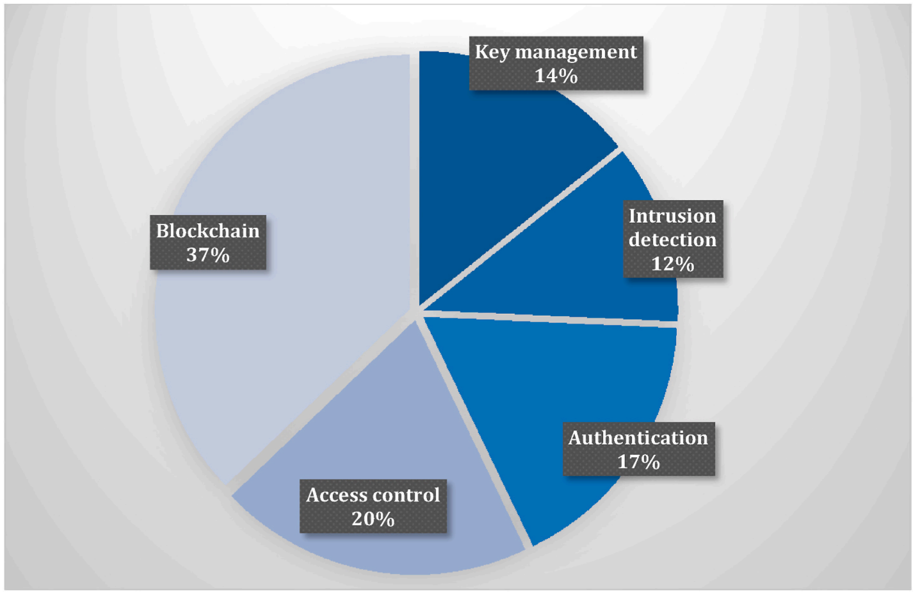

Fig. 12. IoMT Security methods percentage.

Table 4
IoMT security requirements and methods.

Security	Confidentiality	Integrity	Availability	Authenticity
Key management methods	Kaushik et al. (2019); Sun et al. (2019); Zhang et al., 2018			Shen et al. (2018); Suresh (2019)
Intrusion detection methods		Hoa (2011); Bostami et al. (2019); Rahman and Mohsenian-Rad (2012)		Meng et al. (2020)
Authentication methods	Sun et al. (2019)	Sun et al. (2019)	Yaacoub et al., 2020); Sun et al. (2019); Rathore et al. (2019)	Xu et al. (2019); Aghili et al. (2019)
Access control methods				Luo et al. (2018); Fahim et al. (2019); Kumar et al. (2017); Mohsin et al. (2019); Hamidi (2018); Hossain et al. (2018); Yang (2018)
Blockchain methods	Niu et al. (2020); Hussein et al. (2018)	Wang et al. (2020); Xia (2017); Daraghmi et al. (2019); Liu et al. (2019); Chen et al. (2019); Shen et al. (2019)		Luo et al. (2018); Yang (2020); Guo et al. (2019); Nguyen et al. (2019); Xu et al. (2019)
Ratio	17%	29%	6%	48%

greatly increases the availability and dissemination of knowledge. Hence the reporting has the potential to spread as misinformation or fake news (Lai et al., 2020). Governments should be responsible for providing accurate knowledge and clarifying misinformation to help the public cope with this novel infection. The situation must be monitored closely, as the more we can learn about this novel virus and its associated outbreak, the better we can respond. Information openness among nations regarding the COVID-19 mitigation will ensure better information collaboration in the event of such pandemic disasters.

7. IoMT security

According to a recent study (Palandrani, 2020), more than 90% of all IoT device transmission is unencrypted, implying that 57% of IoT devices are vulnerable to attacks exposing confidential information. Cyber attacks are not only detrimental to the system but may also pose a danger to human life. Potentially, any cyber-attack may have a drastic impact, risking the life of patients (Yaacoub et al., 2020; Yaqoob et al., 2019).

The rapid evolution and adoption of IoMT, especially in pandemic times, may raise further security concerns, thus preserving the privacy of critical and sensitive medical data becomes more challenging. Numerous attacks, threats, and risks can affect different layers of the IoMT architecture. Hence an IoMT ecosystem must adhere to strict security and privacy specifications (Yaacoub et al., 2020; Yaqoob et al., 2019). stressed that IoMT suffers from security and privacy issues, and enhancements are needed. Approaches such as cryptographic or non-cryptographic algorithms for efficient intrusion detection and prevention are needed. The work of (Wazid et al., 2019) has revealed several malware attacks on IoMT systems, targeting the security requirements, namely data confidentiality, integrity, authenticity, to data availability. The current strategy for security methods has generally emphasized key management, intrusion detection, authentication, and access control (Makhdoom et al., 2019). Fig. 12 shows IoMT security methods percentage, while Table 4 summarizes the IoMT security requirements and recent methods.

In an IoMT application, safety plays a crucial role as it can adversely influence the physiological, psychological, and biological state of human beings. This might also result in the loss of life and limb. For example, assaults on implantable devices, such as brain implants, have been reported to lead to death (Nanayakkara et al., 2019; Rathore et al., 2019). The US Food & Drug Administration (FDA) has recently revised the electronic safety guidelines on medical equipment applications of 2018 with updated advice on securing patient data on such devices and systems (Sun et al., 2019). Cyber threats on medical systems and hospitals are still on the rise, with IoT-based healthcare organizations and

Table 5
IoMT most common cyber attacks.

Attack	Attack vector	Reference
DoS attacks	Cloud Services, Databases	Rathore et al. (2019); Sun et al. (2019); Yaacoub et al. (2020); Yaqoob et al. (2019)
Injection attacks	Databases	Hao et al. (2011); Bostami et al., (2019)
Data leakage	Messages, Network	Kaushik et al. (2019); Sun et al. (2019); Yaqoob et al. (2019); Sengupta et al. (2019)
Device safety	Hardware, Middleware	Hassan et al. (2019); Yaacoub et al. (2020); Yaqoob et al. (2019); Sengupta et al. (2019)

investors scrambling to identify the most important privacy and to tackle security problems.

The privacy issues of using mobile phones to learn population mobility to support healthcare services during the Ebola outbreak are discussed by Sollins (2018) and Wesolowski et al. (2014). Another research by Yasaka et al. (2020) also discussed privacy concerns regarding tracking contacts during disease outbreaks. According to these studies, however, geo-location of people can help to indicate the intensity of infection, but the cell tower location information must be accessible for the Ministry of Health, not the collection of data for public access. According to (Nanayakkara et al., 2019), a study conducted by security analysts found more than 68,000 online medical services with 12,000 of them belonging to a single healthcare organization. All these devices were in danger of cyber-attacks. Even the former US Vice President, Dick Cheney, removed the wireless capability of his heart implant due to concerns on possible life-threatening cyber attacks that might be made through the implanted device (Peterson, 2013). Famous known IoMT cyber attacks are Denial-of-Service (DoS) attacks, Injection attacks, data leakage, and IoMT physical safety, as shown in Table 5.

Denial-of-Service attacks: This type of attack occurs where an IoT system is prevented from uploading patients' health information onto the respective cloud-based services or medical database, or when the healthcare professional is unable to retrieve patient information through the IoMT system. Frequent data backups may be useful in retrieving historical data, but real-time services would be disrupted. Strong authentication on IoMT devices and time stamping may be considered to mitigate the types of attacks (Rathore et al., 2019; Sun et al., 2019; Yaacoub et al., 2020).

Injection Attacks: Data integrity is required to ensure received data has not been corrupted or manipulated in any form throughout communication channels (Hao et al., 2011). An example of such an attack is false data injection attack (Bostami et al., 2019), which has led to false data being transferred to a hospital data center. Another common type of attack is a SQL injection that opens back doors for cybercriminals to gain access to medical databases (Rahman and Mohsenian-Rad, 2012).

Data leakage, privacy & confidentiality: Compilation and storing of an individual's health and movement records should conform to legal and ethical laws on privacy. However, this may prove difficult and somewhat problematic, especially in cases of contact tracing by authorities during pandemic times where the movement of groups of specific individuals will be monitored. Owing to the transparent and accessible nature of wireless messages, IoMT systems are also more likely to suffer from data leakage through sniffing attacks (Kaushik et al., 2019; Sun et al., 2019), and these include eavesdropping, traffic analysis, and brute force attacks.

IoMT sensor/device safety: The immunity and safety of medical devices is the most daunting aspect due to the limited resources and computing power of the IoT hardware. Generic solutions for security problems cannot be implemented as they are typically difficult to enforce on these low powered devices, and hence a lightweight security middleware framework may be more suited (Hassan et al., 2019; Yaacoub et al., 2020).

7.1. Recent technology in securing IoMT

Implementing security on IoMT devices is a challenging task due to the constrained-device criteria and distributed architecture of IoMT ecosystem. Additionally, these devices are located at the edge of a network and, in some cases, are remote or located within the body, etc. and not easily accessible. Moreover, data protection and safe communication that adhere to security requirements are required to make IoMT systems secure. Possible interventions include access control via authentication, key protection, trust protection (Luo et al., 2018), and blockchain technology, among others. Fig. 13 illustrates the interventions and the IoMT security requirements.

7.1.1. Authentication & encryption

Many IoT systems suffer from lack or weak authentication as a result of constraints in hardware, energy consumption, and other computing resources. Unfortunately, this has presented opportunities for cyber attacks.

The work of Sun et al. (2019) considers two types of authentication to maintain security and privacy in an IoMT system, i.e., on personal and on system's servers via device and client authentication. The device authentication is performed to secure/encrypt data and maintain confidentiality and integrity of communications.

A common approach for user authentication at personal servers is the use of biometric security, in IoMT systems, biometrics can easily be obtained from physical and surgical equipment worn or implanted into

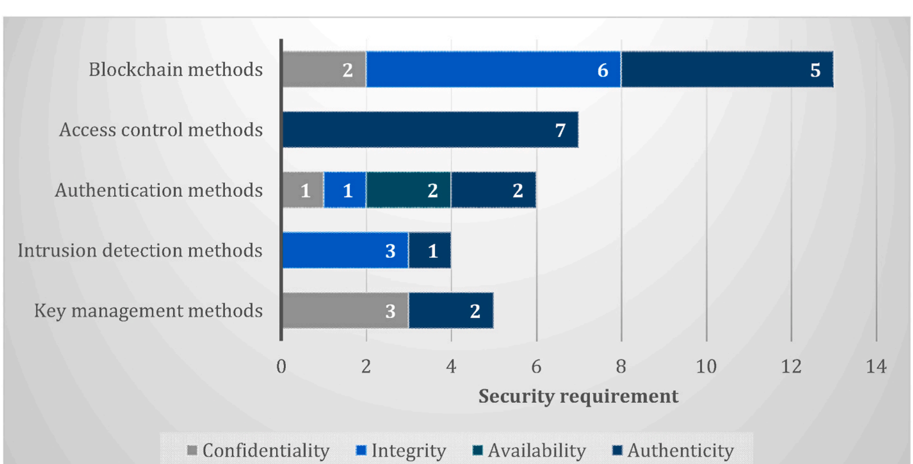

Fig. 13. IoMT security methods and the security requirements.

Table 6
IoMT privacy methods.

Focus Area	Security Requirements	Reference	Privacy Method
Data	Confidentiality	Ting et al., 2020	Two party secure computation protocol
		Luo et al. (2018)	SW-SSS
		Kumar et al. (2017)	Biometric based authentication scheme
		Hassan et al. (2019)	Using Public and Private keys
		Dwivedi et al. (2019)	Proof of Authority, Public Key
Sensor	Resilience to internal attacks	Liu et al. (2019)	MediBchain Nodes Registration
		Kumar et al. (2017)	Biometric based authentication scheme
Cloud	Trust	Liu et al. (2019)	Medical blockchain (MediBchain)
Network	Resistance to man-in-the-middle attack	Liu et al. (2019)	MediBchain
		Hassan et al. (2019)	Privacy preserving strategies of blockchain-based IoT system
End User	Device Authentication	Liu et al., 2019	MediBchain Nodes Registration
	User Authentication	Liu et al. (2019)	MediBchain-Based Privacy-Preserving Mutual Authentication (MBPA)
		Kumar et al. (2017)	Biometric based authentication scheme
		Dwivedi et al. (2019)	Using Public Key and Lightweight Digital Signature
	Patient Anonymity	Hassan et al. (2019)	Removal of Personally Identifiable Information before data publishing
		Dwivedi et al. (2019)	Lightweight Ring Signature
		Yasaka et al. (2020)	Anonymized graph of interpersonal interactions
Administration	Access Control	Kumar et al. (2017)	Biometric based authentication scheme
		Liu et al. (2019)	MBPA
		Dwivedi et al. (2019)	Using Public Key and Lightweight Digital Signature
	Key Management	Luo et al. (2018)	Public-key cryptosystem
	Trust Management	Liu et al. (2019)	MBPA

the human body (Fahim et al., 2019; Kumar et al., 2017; Mohsin et al., 2019). The work of Hamidi (2018) focused on building secure IoMT application access using biometrics as identifiers for secure connections.

In view of hardware constraints, lightweight security approaches like lightweight cryptography, lightweight hybrid anomaly detection, and lightweight multi-factor authentication are possible current approaches to enforce stronger authentication in IoMT systems. In particular (Xu et al., 2019), proposed a secure, lightweight authentication system for WBAN. In this scheme, forward secrecy can be ensured without the use of asymmetric encryption. They believe that their proposed method will greatly minimize computing costs and reduced security risk.

The work of Hossain et al. (2018) focused on a security system that guarantees user authentication via protected access to medical devices by introducing a security access token. The access is cryptographically against forgery and ensures secure access to medical IoT devices (Meng et al., 2020). focused on the detection of malicious devices by designing a trust-based intrusion detection approach based on behavioral profiling of devices in IoMT ecosystem. In another work, Zhang et al. (Zhang et al., 2018) implemented an encrypted medical data that utilized the risk of disease prediction models to preserve privacy.

The work proposed by (Shen et al., 2018) introduced a multilayer authentication protocol for WBAN. The design comprised a multicast group authentication protocol, a new nonpairing cryptographic certificateless authentication protocol, and a group key establishment algorithm with an elliptic-curve cryptography algorithm.

Working on Radio Frequency Identification (RFID) communication (Aghili et al., 2019), demonstrated several attacks such as anonymity, secret disclosure, replay, traceability, and impersonation that may occur within an IoMT system. They then introduced a new mutual RFID authentication protocol to secure communication and preserve the privacy using Burrows–Abadi–Needham (BAN) logic to validate the security features. In addition, the researchers developed an authentication with the ownership transfer protocol for IoMT application to satisfy access control security requirements and preserve privacy. The protocol overcomes de-synchronization, traceability, insider attacks, and DoS. In related work, using the same BAN logic (Sureshkumar et al., 2019), proposed an authenticated key establishment protocol using the Elliptic Curve Cryptography (ECC) to resolve the security problems found in present IoMT communication protocols.

The work of Hussain et al. (2018) highlighted the security and privacy of medical data associated with the Android mobile operating system. A set of security checks and policies was developed that protect against different attacks and malware, as well as disabling intents, permission restrictions, data shadowing, and the impact of enabling/-disabling system peripherals.

Focusing on big data and cloud computing technologies for IoMT, Yang et al. (2018) focused on big data security by developing fine-grained access control manners, a centralized trusted authority, and data encryption using attribute-based encryption.

The privacy requirement at the time of pandemic is a crucial issue, especially with the contact tracing and movement control. Although contact tracing applications are necessary to the authorities, they can leak information about the infected users to third parties, causing serious privacy concerns. Therefore, IoMT users have to develop trust for the centralized servers or use the decentralized approaches provided by blockchain technology. Table 6 shows the IoMT privacy methods and its focus area.

7.1.2. Blockchain

Within the IoMT ecosystem, wearable sensor devices collect and transmit data that contains specific and sometimes considered as sensitive medical data. This data is either stored in local or centralized servers or cloud platforms, which is later used by medical practitioners (nurses, doctors, dieticians, and medical organizations) for diagnosis or treatment regarding various diseases or upcoming threats in the near future.

Blockchain technology helps to improve the privacy of IoMT data as it adopts a naturally decentralized architecture, secured transactions with cryptographic encryption, immutable reliable trust with verifiable transmission backtrack, and easy data (device) identification as it owns unique identifiers. Blockchain technology mitigates the issue of distributed devices with multi-services/platform management, data exchange privacy, transaction tampering, untrusted distributed authorization and authentication services, and untraceable transaction of IoMT devices (Hassan et al., 2019). However, since everything is easily available for each blockchain member, there is a possibility of privacy leakage. Some known blockchain privacy attacks are wallet privacy leakage, address reuse, Sybil attacks, deanonymization, linking attacks, and message spoofing. It is normal for IoMT users to use hospital public Wi-Fi with public addresses, hence, blockchain users are exposed to any adversary that can easily get access to these addresses through unsecured hospital public Wi-Fi.

Blockchain wallets have been introduced to overcome the address reuse issues, whereby temporary disposable addresses are used for each data transmission. Blockchain wallet is a software that handles

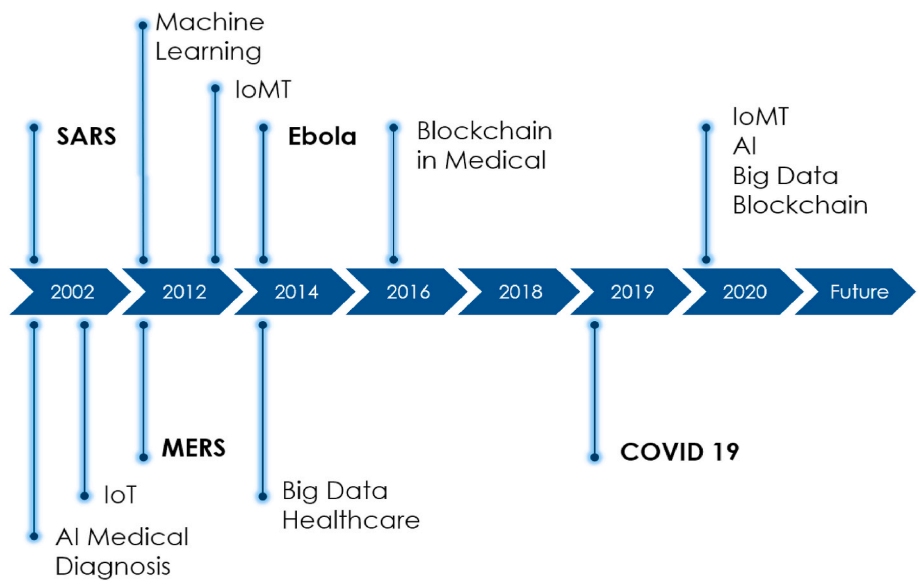

Fig. 14. Timeline for IoMT disease mitigation technology.

addresses transparently, but it has the capability to reveal the privacy of blockchain systems depending on the software security strength. Sybil attacks are when many fake IoMT user nodes are created intentionally to control the IoMT blockchain network. Message spoofing leads to message forgery in the IoMT network to distribute wrong information and diminish the security and privacy of IoMT systems. Linking attack is oriented towards IoMT stored data with the purpose of combining the external data with protected data. In order to overcome these issues, there are few approaches that can be deployed (Hassan et al., 2019), classified the privacy protection of blockchain IoMT systems approaches into two, (i) Preserving privacy for IoMT user identity and (ii) Preserving privacy for IoMT node transmission. General blockchain privacy preservation approaches are encryption, smart contract, anonymization, and differential privacy (Hassan et al., 2019).

Encryption is generally used to protect the privacy of wearable devices. It can only be compromised by mathematically breaking the encryption cipher. (Yang, 2020) developed an encrypted electronic medical data sharing based on blockchain, the encryption is a blend of attribute-based encryption (ABE) and attribute-based signature (ABS). It satisfies the requirements of unforgeability and anonymity and resists

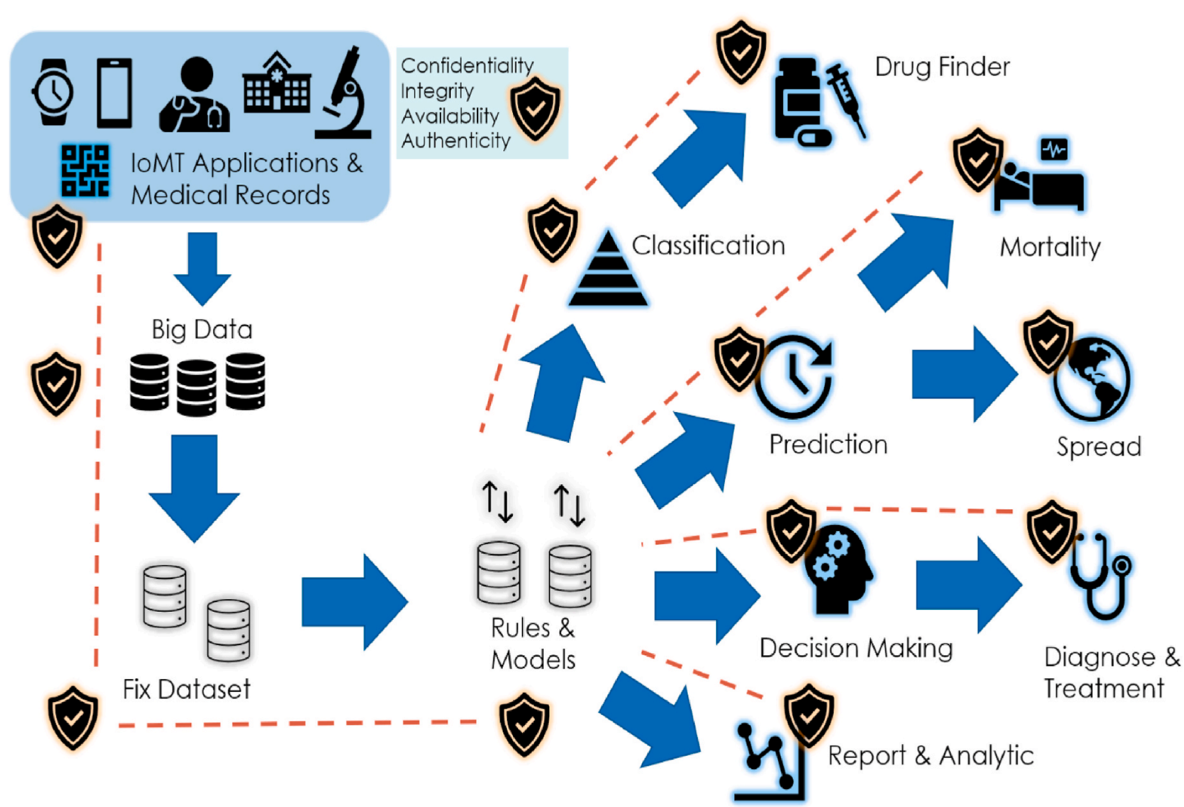

Fig. 15. Secure COVID-19 mitigation ecosystem of IoMT applications and technologies.

chosen cipher attacks (Guo et al., 2019). focused on cloud computing telemedicine system uses blockchain with independent update multi-authority ABE to avoid the misdiagnosis accident caused by malicious attacks from the inner cloud (Niu et al., 2020). proposed a medical data sharing scheme using permissioned blockchains that includes ciphertext ABE for medical data access control and data confidentiality.

Smart contracts use a decentralized nature concept of blockchain. Transaction details are written like a programmable code according to the requirement of the blockchain transaction. The contract gets deployed and executed in the blockchain network (McGhin et al., 2019). (Nguyen et al., 2019) designed a smart contracts trustworthy access control mechanism for medical e-record blockchain and the decentralized interplanetary file system on a mobile cloud platform. (Xia, 2017) employed smart contracts with access control mechanisms in blockchain medical data sharing to avoid violation of data permissions.

Wang et al. (Wang et al., 2020) developed a secure blockchain data transmission and storage method for IoMT interoperating with WBAN. The work focused on medical e-record sharing using consortium blockchain with encryption ciphertext. Specifically, they introduced a cloud-based personal medical record sharing scheme with data integrity verifiable with smart contract combined with searchable symmetric encryption and ABE techniques to achieve privacy protection and fine-grained access control. In another work (Daraghmi et al., 2019), designed a blockchain system to manage medical records with timed-based smart contracts and advanced encryption techniques.

Anonymization is another famous method to preserve privacy in blockchain IoMT applications. Differential privacy is a method that protects IoMT nodes data privacy by adding noise; it uses the dynamic data perturbation concept (Liu et al., 2019). used an elliptic curve computational Diffie-Hellman in a random oracle model to develop a privacy-preserving mobile medical cloud architecture with mutual authentication that supports the patient's anonymity. Messages are dynamically encrypted and integrated to anonymously authenticate nodes.

(Shen et al., 2019) proposed a concept called secure SVM, which is a privacy-preserving SVM training system for blockchain technology-based encrypted IoT data. They used blockchain technologies to create a secure and transparent data storage network between various service providers, where IoT data is encrypted and then registered on a decentralized system. In another work (Chen et al., 2019), focused on the development of a blockchain-based searchable encryption scheme for medical data. The use of blockchain technology ensures the anti-tampering, integrity, and traceability of medical data indices.

(Hussein et al., 2018) implemented a hybrid of blockchain and Discrete Wavelet Transform with Genetic Algorithm in which a blockchain-based data management platform is introduced to resolve privacy issues with medical records. This approach leverages blockchain's immutability and flexibility to effectively overcome access control and sensitive data challenges. They concluded that their method is stable, secure and adaptive. Dwivedi et al. (2019) suggested a new upgraded blockchain architecture that is appropriate for medical IoT devices. This method is dependent on the distributed design and other extra network privacy and security features. This is to provide secure data storage and analysis of healthcare massive data records.

Fig. 14 concluded the technology timeline for IoMT disease mitigation, year 2020 has shown significant increase in the merging of IoMT, Blockchain, Artificial Intelligence, and Big Data for the benefits of human health. While Fig. 15 shows the graphical abstract of the IoMT security, applications and technologies for COVID-19 mitigation.

8. Conclusion

This paper provides a comprehensive overview of IoMT within the context of COVID-19 pandemic in terms of technology development, adoption, and possibilities, and highlights security issues related to IoMT in general. During this pandemic period, a majority of IoMT systems have been used primarily to track and trace infected individuals as digital surveillance, and this has led to some concerns regarding privacy issues - yet this has been regarded as a necessary evil and is accepted by many citizens across the globe. Other applications of IoMT have been in detecting, monitoring, and testing to minimize the risk of infection or to expedite testing procedures. Generally, the same security constraints in IoT would apply to IoMT systems, but since IoMT devices impact human lives, the concern is more pronounced. Hence, in this paper, on-going developments in the realm of IoMT security have been presented extensively, including studies based on newer technologies such as blockchain to lessen security threats to humans and systems. A discussion on the further direction of IoMT in the later part of this paper suggests that hybrid technologies will continue to be developed in the near future, consolidating knowledge from the domains of artificial intelligence, data mining, big data analytics, and IoMT-related technologies for more effective and accurate solutions in automation, simulation, and forecasting. Lastly, it would also be advantageous if these IoMT systems included security as one of the main objectives in their design, thus ensuring a higher degree of safety and privacy for humanity.

Credit author statement

Azana Hafizah Mohd Aman: Writing (original draft, reviewing & editing), Investigation, Visualization, Resource compilation, Project compilation. Wan Haslina Hassan: Writing (original draft, reviewing & editing), Conceptualization, Investigation, Supervision. Shilan Sameen: Writing (original draft), Investigation, Resource compilation. Zainab Senan Attarbashi: Writing (original draft), Investigation. Mojtaba Alizadeh: Writing (original draft), Investigation. Liza Abdul Latiff: Writing (original draft), Investigation.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

The authors are grateful to Universiti Kebangsaan Malaysia, University Teknologi Malaysia, Universiti Utara Malaysia, and Lorestan University for all their support and contribution to this study. This research is funded by research grant FRGS/1/2019/ICT03/UKM/02/1 and GGPM-2019-030.

References

Aghili, S.F., Mala, H., Kaliyar, P., Conti, M., 2019. SecLAP: secure and lightweight RFID authentication protocol for medical IoT. Future Generat. Comput. Syst. 101, 621–634.

Ahad, A., Tahir, M., Yau, K.A., 2019. 5G-Based smart healthcare network: architecture, taxonomy, challenges and future research directions. IEEE Access 7, 100747–100762.

Al-Dhief, F.T., et al., 2020. A survey of voice pathology surveillance systems based on internet of things and machine learning algorithms. IEEE Access 8, 64514–64533.

Alabdulatif, A., Khalil, I., Forkan, A.R.M., Atiquzzaman, M., 2019. Real-time secure health surveillance for smarter health communities. IEEE Commun. Mag. 57 (1), 122–129.

Aliya, S., 2014. CDC Tracks Cell Phone Location Data to Halt Ebola from. https://www.nextgov.com/it-modernization/2014/10/cdc-tracks-cell-phone-location-data-halt-ebola/96239/.

Allam, Z., Jones, D.S., 2020. On the coronavirus (COVID-19) outbreak and the smart city network: universal data sharing standards coupled with artificial intelligence (AI) to benefit urban health monitoring and management. In: Paper Presented at the Healthcare.

Arun, S.S., Neelakanta Iyer, G., 2020. On the analysis of COVID19 - novel corona viral disease pandemic spread data using machine learning techniques. In: 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, pp. 1222–1227.

Baize, S., Pannetier, D., Oestereich, L., Rieger, T., Koivogui, L., Magassouba, N.F., Soropogui, B., Sow, M.S., Keïta, S., De Clerck, H., 2014. Emergence of zaire ebola virus disease in Guinea. N. Engl. J. Med. 371 (15), 1418–1425.

Bell, B.P., 2016. Overview, control strategies, and lessons learned in the CDC response to the 2014–2016 Ebola epidemic. MMWR supplements 65.

Bosch, 2020. Combating the Coronavirus Pandemic: Bosch Develops Rapid Test for COVID-19. https://www.bosch.com/stories/vivalytic-rapid-test-for-covid-19/.

Bostami, B., Ahmed, M., Choudhury, S., 2019. False Data Injection Attacks in Internet of Things. EAI/Springer Innovations in Communication and Computing, pp. 47–58. https://doi.org/10.1007/978-3-319-93557-7_4.

Boulos, M.N.K., 2004. Descriptive review of geographic mapping of severe acute respiratory syndrome (SARS) on the Internet. Int. J. Health Geogr. 3 (1), 2.

Boulos, M.N.K., Geraghty, E.M., 2020. Geographical Tracking and Mapping of Coronavirus Disease COVID-19/severe Acute Respiratory Syndrome Coronavirus 2 (SARS-CoV-2) Epidemic and Associated Events Around the World: How 21st Century GIS Technologies Are Supporting the Global Fight against Outbreaks and Epidemics. BioMed Central.

Braden, C.R., Dowell, S.F., Jernigan, D.B., Hughes, J.M., 2013. Progress in global surveillance and response capacity 10 years after severe acute respiratory syndrome. Emerg. Infect. Dis. 19 (6), 864.

Briand, S., Bertherat, E., Cox, P., Formenty, P., Kieny, M.-P., Myhre, J.K., Roth, C., Shindo, N., Dye, C., 2014. The international Ebola emergency. N. Engl. J. Med. 371 (13), 1180–1183.

Busvine, D., 2020. Covid-19: Germany Launches Smartwatch App to Monitor Coronavirus Spread from. https://www.thestar.com.my/tech/tech-news/2020/04/07/covid-19-germany-launches-smartwatch-app-to-monitor-coronavirus-spread.

Buurman, B., Kamruzzaman, J., Karmakar, G., Islam, S., 2020. Low-power wide-area networks: design goals, architecture, suitability to use cases and research challenges. IEEE Access 8, 17179–17220.

Cao, R., Tang, Z., Liu, C., Veeravalli, B., 2020. A scalable multicloud storage architecture for cloud-supported medical internet of things. IEEE Internet of Things Journal 7 (3), 1641–1654.

Cascella, M., Rajnik, M., Cuomo, A., Dulebohn, S.C., Di Napoli, R., 2020. Features, evaluation and treatment coronavirus (COVID-19). StatPearls [Internet]. StatPearls Publishing.

CDC, 2003. Severe Acute Respiratory Syndrome: Fact Sheet; Basic Information about SARS. Retrieved from. http://www.cdc.gov/ncidod/sars/factsheet.

CDC, 2015. Fact Sheet about Middle East Respiratory Syndrome (MERS). Retrieved from USA. https://www.cdc.gov/coronavirus/mers/about/index.html.

Chen, L., Lee, W.-K., Chang, C.-C., Choo, K.-K.R., Zhang, N., 2019. Blockchain based searchable encryption for electronic health record sharing. Future Generat. Comput. Syst. 95, 420–429.

Chinazzi, et al., 2020. The effect of travel restrictions on the spread of the 2019 novel coronavirus (COVID-19) outbreak. Science 368 (6489), 395–400.

Chowell, G., Nishiura, H., 2015. Characterizing the transmission dynamics and control of ebola virus disease. PLoS Biol. 13 (1).

Christaki, E., 2015. New technologies in predicting, preventing and controlling emerging infectious diseases. Virulence 6 (6), 558–565.

Consulting, V.W., 2009. mHealth for Development: the Opportunity of Mobile Technology for Healthcare in the Developing World. Washington Dc and Berkshire, UK.

Control, C.f.D., Prevention, 2020. 2019-2020 US Flu Season: Preliminary Burden Estimates.

Daraghmi, E., Daraghmi, Y., Yuan, S., 2019. MedChain: a design of blockchain-based system for medical records access and permissions management. IEEE Access 7, 164595–164613.

Dimitrov, D.V., 2016. Medical internet of things and big data in healthcare. Healthcare informatics research 22 (3), 156–163.

Din, I.U., Guizani, M., Hassan, S., Kim, B.S., Khan, M.K., Atiquzzaman, M., 2018. The Internet of Things: a review of enabled technologies and future challenges. IEEE Access 7, 7606–7640.

Djama, A., Djamaa, B., Senouci, M.R., 2020. Information-Centric Networking solutions for the Internet of Things: a systematic mapping review. Comput. Commun. 159 (2020), 37–59.

Dwivedi, A.D., Srivastava, G., Dhar, S., Singh, R., 2019. A decentralized privacy-preserving healthcare blockchain for IoT. Sensors 19 (2), 326.

D'Silva, J.P., Eisenberg, M.C., 2015. Modeling spatial transmission of ebola in West Africa arXiv preprint arXiv:1507.08367.

Fahim, S.R., Shahriar, S., Islam, O.K., Rahman, M.I., Sarker, S.K., Akter, S., 2019. Development of a remote tracking security box with multi-factor Authentication system incorporates with a biometric sensing device. In: 2019 IEEE International WIE Conference on Electrical and Computer Engineering (WIECON-ECE). IEEE.

Fähnrich, C., Denecke, K., Adeoye, O., Benzler, J., Claus, H., Kirchner, G., Mall, S., Richter, R., Schapranow, M., Schwarz, N.G., 2015. Surveillance and outbreak response management system (SORMAS) to support the control of the ebola virus disease outbreak in West Africa. Euro Surveill. 20 (12), 21071.

Fan, Q., Yao, X.A., Dang, A., 2020. Spatiotemporal Analysis and Data Mining of the 2014–2016 Ebola Virus Disease Outbreak in West Africa. Geospatial Technologies for Urban Health. Springer, pp. 181–208.

Ferretti, L., et al., 2020. Quantifying dynamics of sars-cov-2 transmission suggests that epidemic control with digital contact tracing. Science 31, eabb6936. https://doi.org/10.1126/science.abb6936. Mar 2020.

Georgi, N., Corvol, A., Jeannas, R.L.B., 2018. Middleware architecture for health sensors interoperability. IEEE Access 6, 26283–26291.

Gostin, L.O., 2018. New Ebola outbreak in Africa is a major test for the WHO. Jama 320 (2), 125–126.

Green, A., 2017. Ebola outbreak in the DR Congo. Lancet 389 (10084), 2092.

Gu, F., Niu, J., Jiang, L., Liu, X., Atiquzzaman, M., 2020. Survey of the low power wide area network technologies. J. Netw. Comput. Appl. 149, 102459.

Guo, R., Shi, H., Zheng, D., Jing, C., Zhuang, C., Wang, Z., 2019. Flexible and efficient blockchain-based ABE scheme with multi-authority for medical on demand in telemedicine system. IEEE Access 7, 88012–88025.

Hameed, S.S., Hassan, R., Muhammad, F.F., 2017. Selection and classification of gene expression in autism disorder: use of a combination of statistical filters and a GBPSO-SVM algorithm. PloS One 12 (11).

Hamidi, H., 2018. An approach to develop the smart health using Internet of Things and authentication based on biometric technology. Future Generat. Comput. Syst. 91, 434–449.

Hao, Z., Zhong, S., Yu, N., 2011. A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability. IEEE Trans. Knowl. Data Eng. 23 (9), 1432–1437.

Hassan, M.U., Rehmani, M.H., Chen, J., 2019. Privacy preservation in blockchain based IoT systems: integration issues, prospects, challenges, and future research directions. Future Generat. Comput. Syst. 97, 512–529.

Her, M., 2020. How is COVID-19 affecting South Korea? What is our current strategy? Disaster Med. Public Health Prep. 1–3.

Homaei, M.H., Salwana, E., & Shamshirband, S. An enhanced distributed data aggregation method in the internet of things. Sensors, 19, 3173.

Hossain, M., Islam, S.M.R., Ali, F., Kwak, K.-S., Hasan, R., 2018. An Internet of Things-based health prescription assistant and its security system design. Future Generat. Comput. Syst. 82, 422–439.

Hosseini, E., Ghafoor, K., Sadiq, A., Guizani, M., Emrouznejad, A., 2020. COVID-19 optimizer algorithm, modeling and controlling of coronavirus distribution process. IEEE Journal of Biomedical and Health Informatics. https://doi.org/10.1109/JBHI.2020.3012487.

Hui, M., 2020. How Taiwan Is Tracking 55,000 People under Home Quarantine in Real Time. Retrieved from. https://qz.com/1825997/taiwan-phone-tracking-system-monitors-55000-under-coronavirus-quarantine/.

Hussain, M., Al-Haiqi, A., Zaidan, A.A., Zaidan, B.B., Kiah, M., Iqbal, S., Abdulnabi, M., 2018. A security framework for mHealth apps on Android platform. Comput. Secur. 75, 191–217.

Hussein, A.F., ArunKumar, N., Ramirez-Gonzalez, G., Abdulhay, E., Tavares, J.M.R., de Albuquerque, V.H.C., 2018. A medical record managing and securing blockchain based system supported by a genetic algorithm and discrete wavelet transform. Cognit. Syst. Res. 52, 1–11.

IEEE Standard Association. Retrieved date. https://standards.ieee.org/standard/2413-2019.html. (Accessed 20 April 2020).

Inn, T.L., 2020. Smart City Technologies Take on COVID-19. World Health.

Islam, S.M.R., Kwak, D., Kabir, M.H., Hossain, M., Kwak, K., 2015. The internet of things for health care: a comprehensive survey. IEEE Access 3, 678–708.

Jamrisko, M.W.L., 2020. Germany breaks Korea's six-year streak as most innovative nation. from. https://www.bloomberg.com/news/articles/2020-01-18/germany-breaks-korea-s-six-year-streak-as-most-innovative-nation.

Jia, L., Li, K., Jiang, Y., Guo, X., 2020. Prediction and Analysis of Coronavirus Disease 2019 arXiv preprint. 2003.05447.

Karimuribo, E.D., Mutagahywa, E., Sindato, C., Mboera, L., Mwabukusi, M., Njenga, M. K., Teesdale, S., Olsen, J., Rweyemamu, M., 2017. A smartphone app (AfyaData) for innovative one health disease surveillance from community to national levels in Africa: intervention in disease surveillance. JMIR public health and surveillance 3 (4), e94.

Kaushik, I., Sharma, N., Singh, N., 2019. Intrusion detection and security system for blackhole attack. In: 2019 2nd International Conference on Signal Processing and Communication (ICSPC). IEEE.

Koh, D., 2020. Temp Pal Smart Thermometer Helps Reduce COVID-19 Spread in Hospitals. Retrieved from. https://www.mobihealthnews.com/news/asia-pacific/temp-pal-smart-thermometer-helps-reduce-covid-19-spread-hospitals.

Kramer, A.M., Pulliam, J.T., Alexander, L.W., Park, A.W., Rohani, P., Drake, J.M., 2016. Spatial spread of the West Africa ebola epidemic. Royal Society open science 3 (8), 160294.

Kumar, T., Braeken, A., Liyanage, M., Ylianttila, M., 2017. Identity privacy preserving biometric based authentication scheme for naked healthcare environment. In: 2017 IEEE International Conference on Communications (ICC). IEEE.

Lai, C.-C., Shih, T.-P., Ko, W.-C., Tang, H.-J., Hsueh, P.-R., 2020. Severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) and corona virus disease-2019 (COVID-19): the epidemic and the challenges. Int. J. Antimicrob. Agents 105924. https://doi.org/10.1016/j.ijantimicag.2020.105924.

Lee, Y., 2020. Covid-19: Taiwan's New 'electronic Fence' for Quarantines Leads Wave of Virus Monitoring. Retrieved from. https://www.thestar.com.my/tech/tech-news/2020/03/20/covid-19-taiwans-new-electronic-fence-for-quarantines-leads-wave-of-virus-monitoring.

Leggiadro, R.J., 2019. Outbreaks in a rapidly changing central Africa: lessons from ebola. Pediatr. Infect. Dis. J. 38 (1), 88.

Leite, H., Gruber, T., Hodgkinson, I.R., 2019. Flattening the infection curve – understanding the role of telehealth in managing COVID-19. Leader. Health Serv. 33 (2), 1751–1879. https://doi.org/10.1108/LHS-05-2020-084.

Limaye, T.A., 2018. HERMIT: a benchmark suite for the internet of medical things. IEEE Internet of Things Journal 5 (5), 4212–4222.

Liu, C., Chen, F., Zhao, C., Wang, T., Zhang, C., Zhang, Z., 2018. IPv6-Based architecture of community medical internet of things. IEEE Access 6, 7897–7910.

Liu, X., Ma, W., Cao, H., 2019. MBPA: a medibchain-based privacy-preserving mutual authentication in TMIS for mobile medical cloud architecture. IEEE Access 7, 149282–149298.

Louis, M.S., 2012. Global health surveillance. MMWR Surveill Summ 61 (Suppl. l), 15–19.
Luo, E., Bhuiyan, M.Z.A., Wang, G., Rahman, M.A., Wu, J., Atiquzzaman, M., 2018. Privacyprotector: privacy-protected patient data collection in IoT-based healthcare systems. IEEE Commun. Mag. 56 (2), 163–168.
Ma, Y., Wang, Y., Yang, J., Miao, Y., Li, W., 2017. Big health application system based on health internet of things and big data. IEEE Access 5, 7885–7897.
Makhdoom, I., Abolhasan, M., Abbas, H., Ni, W., 2019. Blockchain's adoption in IoT: the challenges, and a way forward. J. Netw. Comput. Appl. 125, 251–279.
Marjani, M., Nasaruddin, F., Gani, A., Karim, A., Hashem, I.A.T., Siddiqa, A., Yaqoob, I., 2017. Big IoT data analytics: architecture, opportunities, and open research challenges. IEEE Access 5, 5247–5261.
Massaro, E., Kondor, D., Ratti, C., 2019. Assessing the interplay between human mobility and mosquito borne diseases in urban environments. Sci. Rep. 9 (1), 16911.
McGhin, T., Choo, K.K.R., Liu, C.Z., He, D., 2019. Blockchain in healthcare applications: research challenges and opportunities. J. Netw. Comput. Appl. 135, 62–75.
Meng, W., Li, W., Wang, Y., Au, M.H., 2020. Detecting insider attacks in medical cyber–physical networks based on behavioral profiling. Future Generat. Comput. Syst. 108, 1258–1266.
Miao, Y., Wu, G., Liu, C., Hossain, M.S., Muhammad, G., 2019. Green cognitive body sensor network: architecture, energy harvesting, and smart clothing-based applications. IEEE Sensor. J. 19 (19), 8371–8378 (2019).
Microsoft, 2020. Trying to Shield Hospital Staff and Patients from COVID-19 with Help from AI, Cloud, and Intelligent Edge - Asia News Center. Retrieved from. https://news.microsoft.com/apac/2020/03/31/trying-to-shield-hospital-staff-and-patients-from-covid-19-with-help-from-ai-cloud-and-intelligent-edge/.
Ministry of Health and Welfare, 2020. S.Korea's Secret Weapon against COVID-19. Explained by 13 Frontline Workers, video viewed at. http://ncov.mohw.go.kr/en/duBoardList.do?brdId=12&brdGubun=121&dataGubun=&ncvContSeq=&contSeq=&board_id=&gubun=.
Mohammed, M.A., et al., 2020. Benchmarking methodology for selection of optimal COVID-19 diagnostic model based on entropy and TOPSIS methods. IEEE Access 8, 99115–99131.
Mohd Aman, A.H., Yadegaridehkordi, E., Attarbashi, Z.S., Hassan, R., Park, Y., 2020. A survey on trend and classification of internet of things reviews. IEEE Access 8, 111763–111782.
Mohsin, A., Zaidan, A., Zaidan, B., Albahri, O., Albahri, A., Alsalem, M., Mohammed, K., 2019. Based Blockchain-PSO-AES techniques in finger vein biometrics: a novel verification secure framework for patient authentication. Comput. Stand. Interfac. 66, 103343.
Momattin, H., Mohammed, K., Zumla, A., Memish, Z.A., Al-Tawfiq, J.A., 2013. Therapeutic options for Middle East respiratory syndrome coronavirus (MERS-CoV)–possible lessons from a systematic review of SARS-CoV therapy. Int. J. Infect. Dis. 17 (10), e792–798.
Moon, G., 2020. South Korea's Return to Normal Interrupted by Uptick in Coronavirus Cases. Accessed at. https://www.nbcnews.com/news/world/south-korea-s-return-normal-interrupted-uptick-coronavirus-cases-n1176021. (Accessed 28 April 2020).
Nanayakkara, N., Halgamuge, M., Syed, A., 2019. Security and Privacy of Internet of Medical Things (IoMT) Based Healthcare Applications: A Review.
Nguyen, D.C., Pathirana, P.N., Ding, M., Seneviratne, A., 2019. Blockchain for secure EHRs sharing of mobile cloud based E-health systems. IEEE Access 7, 66792–66806.
Niu, S., Chen, L., Wang, J., Yu, F., 2020. Electronic health record sharing scheme with searchable attribute-based encryption on blockchain. IEEE Access 8, 7195–7204.
Noh, J.W., Yoo, K.B., Kwon, Y.D., Hong, J.H., Lee, Y., Park, K., 2020. Effect of information disclosure policy on control of infectious disease: MERS-CoV outbreak in South Korea. Int. J. Environ. Res. Publ. Health 17 (1).
Noor, M.M., Hassan, W.H., 2019. Current research on internet of things (IoT) security: a survey. Comput. Network. 148, 283–294.
Nour, B., Ibn Khedher, H., Moungla, H., Afifi, H., Li, F., Kashif, S., et al., 2019. Internet of things mobility over information-centric/named-data networking. IEEE Internet Computing 24 (1), 14–24.
Olesch, A., 2020. Germany Benefits from Digital Health Infrastructure during COVID-19 Pandemic from. https://www.healthcareitnews.com/news/europe/germany-benefits-digital-health-infrastructure-during-covid-19-pandemic.
Pace, P., Aloi, G., Gravina, R., Caliciuri, G., Fortino, G., Liotta, A., 2019. An edge-based architecture to support efficient applications for healthcare industry 4.0. IEEE Transactions on Industrial Informatics 15 (1), 481–489.
Palandrani, P., 2020. How Cybersecurity Will Accelerate IoT's Growth. Retrieved from. https://www.globalxetfs.com/how-cybersecurity-will-accelerate-iots-growth/.
Pandey, R., Gautam, V., Bhagat, K., Sethi, T., 2020. A Machine Learning Application for Raising WASH Awareness in the Times of Covid-19 Pandemic arXiv preprint. 2003.07074.
Paraguassu, E.C., Chen, H., Zhou, F., Xu, Z., Wang, M., 2020. Coronavirus and COVID-19: the latest news and views from the scientific community about the new coronavirus and COVID-19. Brazilian Journal of Implantology and Health Sciences 2 (3), 96–109.
Peeri, N.C., Shrestha, N., Rahman, M.S., Zaki, R., Tan, Z., Bibi, S., Haque, U., 2020. The SARS, MERS and novel coronavirus (COVID-19) epidemics, the newest and biggest global health threats: what lessons have we learned? Int. J. Epidemiol.
Peterson, A., 2013. Yes, terrorists could have hacked Dick Cheney's heart. Wash. Post 21 (10).
Poletto, C., Gomes, M.F., Piontti, A.P., Rossi, L., Bioglio, L., et al., 2014. Assessing the impact of travel restrictions on international spread of the 2014 West African Ebola epidemic. Euro Surveill.: bulletin Europeen sur les maladies transmissibles= European communicable disease bulletin 19 (42).
Pramanik, M.I., Lau, R.Y., Demirkan, H., Azad, M.A.K., 2017. Smart health: big data enabled health paradigm within smart cities. Expert Syst. Appl. 87, 370–383.
Rahman, M.A., Mohsenian-Rad, H., 2012. False data injection attacks with incomplete information against smart power grids. In: 2012 IEEE Global Communications Conference (GLOBECOM). IEEE.
Rahman, M.S., Peeri, N.C., Shrestha, N., Zaki, R., Haque, U., Hamid, S.H.A., 2020. Defending against the novel coronavirus (COVID-19) outbreak: how can the internet of things (IoT) help to save the World? Health Policy and Technology. https://doi.org/10.1016/j.hlpt.2020.04.005.
Randrianasolo, L., Raoelina, Y., Ratsitorahina, M., Ravolomanana, L., Andriamandimby, S., et al., 2010. Sentinel surveillance system for early outbreak detection in Madagascar. BMC Publ. Health 10 (1), 31.
Rathee, G., Sharma, A., Kumar, R., Ahmad, F., Iqbal, R., 2019. A trust management scheme to secure mobile information centric networks. Comput. Commun. 151 (2020), 66–75.
Rathore, H., Al-Ali, A.K., Mohamed, A., Du, X., Guizani, M., 2019. A novel deep learning strategy for classifying different attack patterns for deep brain implants. IEEE Access 7, 24154–24164.
Rogoff, K., 2020. Mapping Covid-19 Global Recession. https://www.project-syndicate.org/commentary/mapping-covid19-global-recession-worst-in-150-years-by-kenneth-rogoff-2020-04.
Saheb, T., Izadi, L., 2019. Paradigm of IoT big data analytics in healthcare industry: a review of scientific literature and mapping of research trends. Telematics Inf.
Sandhu, R., Sood, S.K., Kaur, G., 2016. An intelligent system for predicting and preventing MERS-CoV infection outbreak. J. Supercomput. 72 (8), 3033–3056.
Sareen, S., Sood, S.K., Gupta, S.K., 2016. IoT-based cloud framework to control Ebola virus outbreak. Journal of Ambient Intelligence and Humanized Computing 9 (3), 459–476.
Sengupta, J., Ruj, S., Bit, S.D., 2019. A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. J. Netw. Comput. Appl. 149, 102481.
Shahidul Islam, M., Islam, M.T., Almutairi, A.F., Beng, G.K., Misran, N., Amin, N., 1884. Monitoring of the human body signal through the internet of things (IoT) based LoRa wireless network system. Appl. Sci. 9.
Shaman, J., Yang, W., Kandula, S., 2014. Inference and forecast of the current west african ebola outbreak in Guinea, Sierra Leone and Liberia. PLoS currents 6.
Shen, J., Chang, S., Shen, J., Liu, Q., Sun, X., 2018. A lightweight multi-layer authentication protocol for wireless body area networks. Future Generat. Comput. Syst. 78, 956–963.
Shen, M., Tang, X., Zhu, L., Du, X., Guizani, M., 2019. Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities. IEEE Internet of Things Journal 6 (5), 7702–7712.
Sheng, T.J., et al., 2020. An internet of things based smart waste management system using LoRa and tensorflow deep learning model. IEEE Access 8, 148793–148811.
Shim, E., Tariq, A., Choi, W., Lee, Y., Chowell, G., 2020. Transmission potential and severity of COVID-19 in South Korea. Int. J. Infect. Dis. 93, 339–344.
Sokouti, M., Sadeghi, R., Pashazadeh, S., Eslami, S., Sokouti, M., Ghojazadeh, M., Sokouti, B., 2020. Comparative global epidemiological investigation of SARS-CoV-2 and SARS-CoV diseases using meta-MUMS tool through incidence, mortality, and recovery rates. Arch. Med. Res. https://doi.org/10.1016/j.arcmed.2020.04.005.
Sollins, K.R., 2018. IoT big data security and privacy vs. Innovation. IEEE Internet Things Journal 6 (2), 1628–1635.
Song, Y., Jiang, J., Wang, X., Yang, D., Bai, C., 2020. Prospect and application of Internet of Things technology for prevention of SARIs. Clinical eHealth 3, 1–4. https://doi.org/10.1016/j.ceh.2020.02.001.
Sun, Y., Lo, F.P.-W., Lo, B., 2019. Security and privacy for the internet of medical things enabled healthcare systems: a survey. IEEE Access 7, 183339–183355.
Taiwanese Public Opinion Foundation, 2020. February 2020 "Wuhan Pneumonia, Government Efficacy and Cross-Strait Relations. -Taiwan Public Opinion Education Foundation. Retrieved from. https://www.tpof.org.
Team, W.E.R., 2014. Ebola virus disease in West Africa—the first 9 months of the epidemic and forward projections. N. Engl. J. Med. 371 (16), 1481–1495.
Telionis, P.A., Corbett, P., Venkatramanan, S., Lewis, B., 2020. Methods for rapid mobility estimation to support outbreak response. Health security 18 (1), 1–15.
Ting, D.S.W., Carin, L., Dzau, V., Wong, T.Y., 2020. Digital technology and COVID-19. Nat. Med. 26, 7.
Tom-Aba, D., Nguku, P.M., Arinze, C.C., Krause, G., 2018. Assessing the concepts and designs of 58 mobile apps for the management of the 2014-2015 West Africa Ebola outbreak: systematic review. JMIR public health and surveillance 4 (4), e68.
Tsai, I.-W., 2020. President of Taiwan: How My Country Prevented a Major Outbreak of COVID-19. Retrieved from. https://time.com/collection-post/5820596/taiwan-coronavirus-lessons/.
Tseng, T.W., Wu, C.T., Lai, F., 2019. Threat analysis for wearable health devices and environment monitoring internet of things integration system. IEEE Access 7, 144983–144994.
Uddin, M.A., Stranieri, A., Gondal, I., Balasubramanian, V., 2018. Continuous patient monitoring with a patient centric agent: a block Architecture. IEEE Access 6, 32700–32726.
US embassy Consultant, 2020. COVID-19 Information.
Vaishya, R., Javaid, M., Khan, I.H., Haleem, A., 2020. Artificial Intelligence (AI) applications for COVID-19 pandemic. Diabetes & Metabolic Syndrome: Clinical Research & Reviews.
Vinitha, S., Sweetlin, S., Vinusha, H., Sajini, S., 2018. Disease prediction using machine learning over big data. Comput. Sci. Eng.: An International Jouranl (CSEIJ) 8 (1).
Wang, J.C., Ng, C.Y., Brook, R.H., 2020. Response to COVID-19 in taiwan: big data analytics, new technology, and proactive testing. J. Am. Med. Assoc. 323 (14), 2.
Wazid, M., Das, A.K., Rodrigues, J.J.P.C., Shetty, S., Park, Y., 2019. IoMT malware detection approaches: analysis and research challenges. IEEE Access 7, 182459–182476.

Wei, K., Zhang, L., Guo, Y., Jiang, X., 2020. Health monitoring based on internet of medical things: architecture, enabling technologies, and applications. IEEE Access 8, 27468–27478.
Wesolowski, A., Buckee, C.O., Bengtsson, L., Wetter, E., Lu, X., Tatem, A.J., 2014. Commentary: containing the Ebola outbreak-the potential and challenge of mobile network data. PLoS currents 6.
WHO, 2014a. Contact Tracing during an Outbreak of Ebola Virus Disease.
WHO, 2014b. Ebola virus disease: Cuban medical team heading for Sierra Leone. Retrieved date:[16 November, 2017], Online available at: http://www.who.int/esr/disease/ebola/en.
WHO, 2014c. WHO Statement on the Meeting of the International Health Regulations Emergency Committee Regarding the 2014 Ebola Outbreak in West Africa.
WHO, 2020. Public Health Passenger Locator Card. https://www.who.int/ihr/ports_airports/locator_card/en/.
WorldPop, 2014. WorlPop Datasets and Images for West African Countries Covering Population and Mobility Patterns to Support Efforts in Controlling Ebola Virus Outbreak. WorldPop.
Xu, G., Lan, Y., Zhou, W., Huang, C., Li, W., et al., 2019. An IoT-based framework of webvr visualization for medical big data in connected health. IEEE Access 7, 173866–173874.
Xu, Z., Xu, C., Liang, W., Xu, J., Chen, H., 2019. A lightweight mutual authentication and key agreement scheme for medical Internet of Things. IEEE Access 7, 53922–53931.
Yaacoub, J.-P.A., Noura, M., Noura, H.N., Salman, O., Yaacoub, E., et al., 2020. Securing internet of medical things systems: limitations, issues and recommendations. Future Generat. Comput. Syst. 105, 581–606.
Yan, L., Zhang, H.-T., Goncalves, J., Xiao, Y., Wang, M., Guo, Y., et al., 2020. A Machine Learning-Based Model for Survival Prediction in Patients with Severe COVID-19 Infection. medRxiv.
Yao, T.-T., Qian, J.-D., Zhu, W.-Y., Wang, Y., Wang, G.-Q., 2020. A systematic review of lopinavir therapy for SARS coronavirus and MERS coronavirus-A possible reference for coronavirus disease-19 treatment option. J. Med. Virol. https://doi.org/10.1002/jmv.25729.
Yaqoob, T., Abbas, H., Atiquzzaman, M., 2019. Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices – a review. IEEE Communications Surveys & Tutorials 21 (4), 3723–3768.
Yasaka, T.M., Lehrich, B.M., Sahyouni, R., 2020. Peer-to-Peer contact tracing: development of a privacy-preserving smartphone app. JMIR mHealth and uHealth 8 (4), e18936.
Yavlinsky, A., Lule, S.A., Burns, R., Zumla, A., McHugh, T.D., et al., 2020. Mobile-based and open-source case detection and infectious disease outbreak management systems: a review. Welcome Open Research 5 (37), 37.
Zhang, H., Li, J., Wen, B., Xun, Y., Liu, J., 2018. Connecting intelligent things in smart hospitals using NB-IoT. IEEE Internet of Things Journal 5 (3), 1550–1560.
Zhang, M., Hao, B., Wang, R., Wang, Y., 2020. A pre-caching strategy based on the content relevance of smart device's request in information-centric IoT. IEEE Access 9, 75761–75771.
Zhou, P., Yang, X.L., Wang, X.G., et al., 2020. A pneumonia outbreak associated with a new coronavirus of probable bat origin. Nature 579 (7798), 270–273.
Zhu, H., Podesva, P., Liu, X., Zhang, H., Teply, T., Xu, Y., et al., 2019. IoT PCR for pandemic disease detection and its spread monitoring. Sensor. Actuator. B Chem. 127098. https://doi.org/10.1016/j.snb.2019.127098.

Azana Hafizah Mohd Aman received her Ph.D., MSc, and BEng in Computer and Information Engineering from International Islamic University Malaysia. She is currently working as a senior lecturer at Research Center for Cyber Security, Faculty of Information Science and Technology (FTSM), The National University of Malaysia (UKM), Malaysia. Her research areas are computer system & networking, information & network security, IoT, cloud computing, and big data.

Wan Haslina Hassan is an Associate Professor at Malaysia-Japan International Institute of Technology (MJIIT), University Technology Malaysia (UTM). Her qualifications include an MSc in Computation from Oxford University and a Ph.D. in Electrical Engineering from UTM. She is presently leading the Cybersecurity Lab at MJIIT, and her research interests include computer and wireless communications, intelligent architectures for mobility management, industrial cybersecurity, and network security.

Shilan S. Hameed is a Ph.D. student at Malaysia-Japan International Institute of Technology (MJIIT), University Technology Malaysia (UTM). She obtained MSc in Computer Science from University Technology Malaysia (UTM) in 2017, where she has been granted the best student and pro-chancellor awards. She has published several papers in peer-reviewed international journals. Her current research interests include Machine Learning, Big data, Medical IoT, and Cybersecurity.

Zainab Senan Attarbashi is a senior lecturer of Computer Networking at the school of computing, University Utara Malaysia (UUM). She received her BSc (in Electronic and Computer Engineering), MSc, and Ph.D. (in Information and Computer Engineering) degrees from the International Islamic University in Malaysia. Her current research interests are Cyber Security, Info-Centric Networks, Network Mobility, and IoT Connectivity.

Mojtaba Alizadeh received his MSc in Information Security and Ph.D. in Computer Network Security from UTM. He completed his post-doctoral studies at Iran Telecommunication Research Center, Tehran, Iran, as part of a project supported by the Iran National Elite Foundation (Bonyad Melli Nokhbegan). His research interest focuses on cybersecurity. He is currently Head, APA Research Center at Lorestan University (LU-CERT), and is working as an Assistant Professor at the Computer Engineering Department at Lorestan University, Khorramabad, Iran.

Liza Abdul Latiff is a Senior Member of IEEE Inc. and currently attached to Razak Faculty of Technology and Informatics in UTM. She obtained her B. Sc in Electrical Engineering from South Dakota State University USA, Masters in Electrical Engineering (Data Communication) and PhD in Electrical Engineering from UTM. She is the Head of Ubiquitous Broadband Access Network (U-BAN) Research Group, an affiliate member of Wireless Communication Center (WCC), and serves as a Member of IMT & Future Networks Working Group in Malaysia Technical Standards Forum Berhad (MTFSB). Her research interests are computer networking and edge computing, routing protocols and quality of service, mobility management and IoT in Healthcare Industry.